



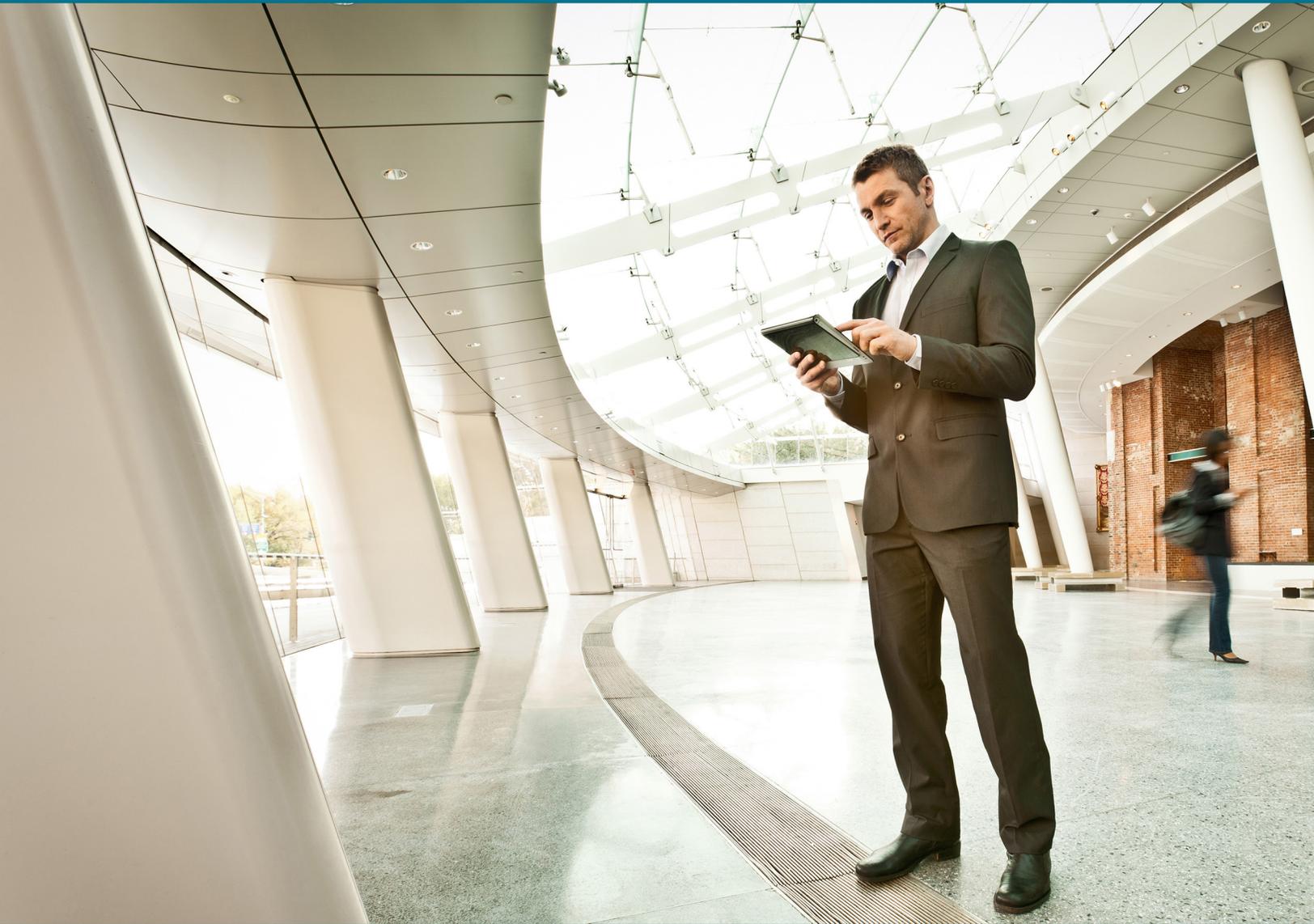
# Newer Cisco Validated Design Guides Available

This guide is part of an older series of Cisco Validated Designs.

Cisco strives to update and enhance CVD guides on a regular basis. As we develop a new series of CVD guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in CVD guides, you should use guides that belong to the same series.

-  [Open the latest version of this guide](#)
-  [Access the latest series of CVD Guides](#)
-  [Continue reading this archived version](#)





# VPN WAN

## Technology Design Guide

December 2013



# Table of Contents

---

<b>Preface</b> .....	<b>1</b>
<b>CVD Navigator</b> .....	<b>2</b>
Use Cases .....	2
Scope .....	2
Proficiency.....	2
<b>Introduction</b> .....	<b>3</b>
Related Reading .....	3
Technology Use Cases .....	3
Use Case: Secure Site-to-Site WAN Communications Using Internet Services.....	3
Design Overview.....	4
WAN Design.....	4
IP Multicast.....	17
Quality of Service .....	17
<b>Deploying the WAN</b> .....	<b>19</b>
Overall WAN Architecture Design Goals.....	19
IP Routing .....	19
LAN Access .....	19
High Availability.....	19
Path Selection Preferences .....	19
Data Privacy (Encryption).....	20
Quality of Service (QoS) .....	20
Design Parameters .....	20
<b>Deploying a DMVPN WAN</b> .....	<b>21</b>
Design Overview.....	21
DMVPN Hub Routers .....	21
Remote Sites–DMVPN Spoke Router Selection.....	22
VRFs and Front Door VRF .....	24
Design Details.....	25
EIGRP .....	27
Encryption .....	28
DMVPN .....	28

Deployment Details .....	30
DMVPN Hub Router Configuration.....	30
Firewall and DMZ Switch Configuration .....	43
Adding DMVPN Hub to Existing WAN-Aggregation Router .....	52
Remote-Site DMVPN Spoke Router Configuration.....	63
Enabling DMVPN Backup on a Remote Site Router .....	78
Router 1 Modifications for Dual Router Design .....	88
Remote-Site DMVPN Spoke Router Configuration (Router 2) .....	95
<b>Deploying a WAN Remote-Site Distribution Layer .....</b>	<b>115</b>
Remote-Site Router to Distribution Layer.....	115
Additional Configuration for Dual Router Design (Router 1) .....	119
Remote-Site Router to Distribution Layer (Router 2) .....	121
<b>Deploying WAN Quality of Service .....</b>	<b>127</b>
QoS Configuration.....	127
<b>Appendix A: Product List .....</b>	<b>133</b>
<b>Appendix B: Technical Feature Supplement .....</b>	<b>137</b>
Front Door VRF (FVRF) for DMVPN .....	137
<b>Appendix C: Device Configuration Files .....</b>	<b>141</b>
<b>Appendix D: Changes.....</b>	<b>142</b>

# Preface

---

Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

## How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64  
ip address 10.5.204.5 255.255.255.0
```

## Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

For the most recent CVD guides, see the following site:

<http://www.cisco.com/go/cvd/wan>

# CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

## Use Cases

This guide addresses the following technology use cases:

- **Secure Site-to-Site WAN Communications Using Internet Services**—Organizations want to securely connect remote sites over public cloud Internet services.

For more information, see the “Use Cases” section in this guide.

## Scope

This guide covers the following areas of technology and products:

- Dynamic Multipoint Virtual Private Network (DMVPN) design and deployment over public WAN transport
- Central-site VPN aggregation and remote-site options for primary and backup communications
- WAN quality of service (QoS) design and configuration

For more information, see the “Design Overview” section in this guide.

## Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNP Routing and Switching**—3 to 5 years planning, implementing, verifying, and troubleshooting local and wide-area networks
- **CCNP Security**—3 to 5 years testing, deploying, configuring, maintaining security appliances and other devices that establish the security posture of the network

## Related CVD Guides



Firewall and IPS Technology Design Guide



MPLS WAN Technology Design Guide



Layer 2 WAN Technology Design Guide

# Introduction

This guide provides guidance and configuration for implementing secure encrypted communications between remote site locations over the Internet using Cisco Dynamic Multipoint VPN technology.

## Related Reading

The [MPLS WAN Technology Design Guide](#) provides flexible guidance and configuration for Multiprotocol Label Switching (MPLS) transport.

The [Layer 2 WAN Technology Design Guide](#) provides guidance and configuration for a VPLS or Metro Ethernet transport.

## Technology Use Cases

Organizations require the WAN to provide sufficient performance and reliability for the remote-site users to be effective in supporting the business. Although most of the applications and services that the remote-site worker uses are centrally located, the WAN design must provide the workforce with a common resource-access experience, regardless of location.

Carrier-based MPLS service is not always available or cost-effective for an organization to use for WAN transport to support remote-site connectivity. Internet-based IP VPNs adequately provide the primary network transport for a remote site. Additionally, they can also provide an optional transport that you can use as a resilient backup to another primary IP VPN. A flexible network architecture should include Internet VPN as a transport option without significantly increasing the complexity of the overall design.

While Internet IP VPN networks present an attractive option for effective WAN connectivity, anytime an organization sends data across a public network there is risk that the data will be compromised. Loss or corruption of data can result in a regulatory violation and can present a negative public image, either of which can have significant financial impact on an organization. Secure data transport over public networks like the Internet requires adequate encryption to protect business information.

### **Use Case: Secure Site-to-Site WAN Communications Using Internet Services**

This guide helps organizations connect remote sites over public cloud Internet services and secure communications between sites.

This design guide enables the following network capabilities:

- Secure, encrypted communications for Internet-based WAN solutions for up to 500 locations by using a hub-and-spoke tunnel overlay configuration
- Deployment as a secondary connectivity solution for resiliency, providing backup to private MPLS WAN service by using single or dual routers in remote locations
- Support for IP Multicast, replication performed on core, hub-site routers
- Compatibility with public cloud solutions where Network Address Translation (NAT) is implemented
- Best-effort quality of service for WAN traffic such as voice over IP and business applications

# Design Overview

The *VPN WAN Technology Design Guide* provides a design that enables highly available, secure, and optimized connectivity for multiple remote-site LANs.

The WAN is the networking infrastructure that provides an IP-based interconnection between remote sites that are separated by large geographic distances.

This document shows you how to deploy the network foundation and services to enable the following:

- VPN WAN connectivity for up to 500 remote sites
- Primary and secondary links to provide redundant topology options for resiliency
- Data privacy via encryption
- Wired LAN access at all remote sites

## WAN Design

The primary focus of the design is to allow usage of the following commonly deployed WAN transport for both primary and secondary links:

- Internet VPN (primary)
- Internet VPN (secondary)

At a high level, the WAN is an IP network, and this transport can be easily integrated to the design. The chosen architecture designates a primary WAN-aggregation site that is analogous to the hub site in a traditional hub-and-spoke design. This site has direct connections to both WAN transports and high-speed connections to the selected service providers. In addition, the site uses network equipment scaled for high performance and redundancy. The primary WAN-aggregation site is coresident with the data center and usually the primary Campus or LAN as well.

This guide also covers the usage of an Internet VPN transport to provide a redundant topology option for a MPLS WAN as configured in the [MPLS WAN Technology Design Guide](#) or Layer 2 WAN resiliency as configured in the [Layer 2 WAN Technology Design Guide](#).

### Internet as WAN Transport

The Internet is essentially a large-scale public WAN composed of multiple interconnected service providers. The Internet can provide reliable high-performance connectivity between various locations, although it lacks any explicit guarantees for these connections. Despite its “best effort” nature, the Internet is a sensible choice for a primary transport when it is not feasible to connect with another transport option. Additional resiliency is provided by using the Internet as an alternate transport option.

Internet connections are typically included in discussions relevant to the Internet edge, specifically for the primary site. Remote-site routers also commonly have Internet connections, but do not provide the same breadth of services using the Internet. For security and other reasons, Internet access at remote sites is often routed through the primary site.

The WAN uses the Internet for VPN site-to-site connections as both a primary WAN transport and as a backup WAN transport (to a primary VPN site-to-site connection).

### Dynamic Multipoint VPN

Dynamic Multipoint VPN (DMVPN) is a solution for building scalable site-to-site VPNs that support a variety of applications. DMVPN is widely used for encrypted site-to-site connectivity over public or private IP networks and can be implemented on all WAN routers used in this design guide.

DMVPN was selected for the encryption solution for the Internet transport because it supports on-demand full mesh connectivity with a simple hub-and-spoke configuration and a zero-touch hub deployment model for adding remote sites. DMVPN also supports spoke routers that have dynamically assigned IP addresses.

DMVPN makes use of multipoint generic routing encapsulation (mGRE) tunnels to interconnect the hub to all of the spoke routers. These mGRE tunnels are also sometimes referred to as DMVPN clouds in this context. This technology combination supports unicast, multicast, and broadcast IP, including the ability to run routing protocols within the tunnels.

## Ethernet WAN

The WAN transports mentioned previously use Ethernet as a standard media type. Ethernet is becoming a dominant carrier handoff in many markets and it is relevant to include Ethernet as the primary media in the tested architectures. Much of the discussion in this guide can also be applied to non-Ethernet media (such as T1/E1, DS-3, OC-3, and so on), but they are not explicitly discussed.

## WAN-Aggregation Designs

The WAN-aggregation (hub) designs include either one or two WAN edge routers. When WAN edge routers are referred to in the context of the connection to a carrier or service provider, they are typically known as *customer edge (CE) routers*. WAN edge routers that terminate VPN traffic are referred to as VPN hub routers. All of the WAN edge routers connect into a distribution layer.

The WAN transport options include traditional Internet access used as either a primary transport, or as a secondary transport when the primary transport is MPLS VPN, Layer 2 WAN or Internet. Only the usage of the Internet transport is documented in this guide. Single or dual carrier Internet access links connect to a VPN hub router or VPN hub router pair, respectively. A similar method of connection and configuration is used for both.

There are multiple WAN-aggregation design models that are documented in this design guide. The DMVPN Only design model uses only Internet VPN as transport. The Dual DMVPN design model uses Internet VPN as both a primary and secondary transport, using dual Internet service providers. Additionally, the DMVPN Backup design models use Internet VPN as a backup to an existing primary MPLS WAN or Layer 2 WAN transport.

The primary difference between the DMVPN backup designs is whether the VPN hub is implemented on an existing MPLS CE router, which is referred to as DMVPN Backup Shared, or the VPN hub is implemented on a dedicated VPN hub router, which is referred to as DMVPN Backup Dedicated.

Each of the design models is shown with LAN connections into either a collapsed core/distribution layer or a dedicated WAN distribution layer. From the WAN-aggregation perspective, there are no functional differences between these two methods.

In all of the WAN-aggregation designs, tasks such as IP route summarization are performed at the distribution layer. There are other various devices supporting WAN edge services, and these devices should also connect into the distribution layer.

The various design models are contrasted in the following tables.

Table 1 - Design models using only VPN transport

	<b>DMVPN Only Design Model</b>	<b>Dual DMVPN Design Model</b>
<b>Remote sites</b>	Up to 100	Up to 500
<b>WAN links</b>	Single	Dual
<b>DMVPN hubs</b>	Single	Dual
<b>Transport 1</b>	Internet VPN	Internet VPN
<b>Transport 2</b>	–	Internet VPN

Table 2 - Design models using VPN transport as backup

	<b>DMVPN Backup Shared Design Model</b>	<b>DMVPN Backup Dedicated Design Model</b>
<b>Remote sites</b>	Up to 50	Up to 500
<b>WAN links</b>	Dual	Multiple
<b>DMVPN hubs</b>	Single (shared with MPLS CE)	Single/Dual
<b>Transport 1 (existing)</b>	MPLS VPN A	MPLS VPN A
<b>Transport 2 (existing)</b>	–	MPLS VPN B
<b>Transport 3 (existing)</b>	–	MetroE/VPLS
<b>Backup transport</b>	Internet VPN	Internet VPN

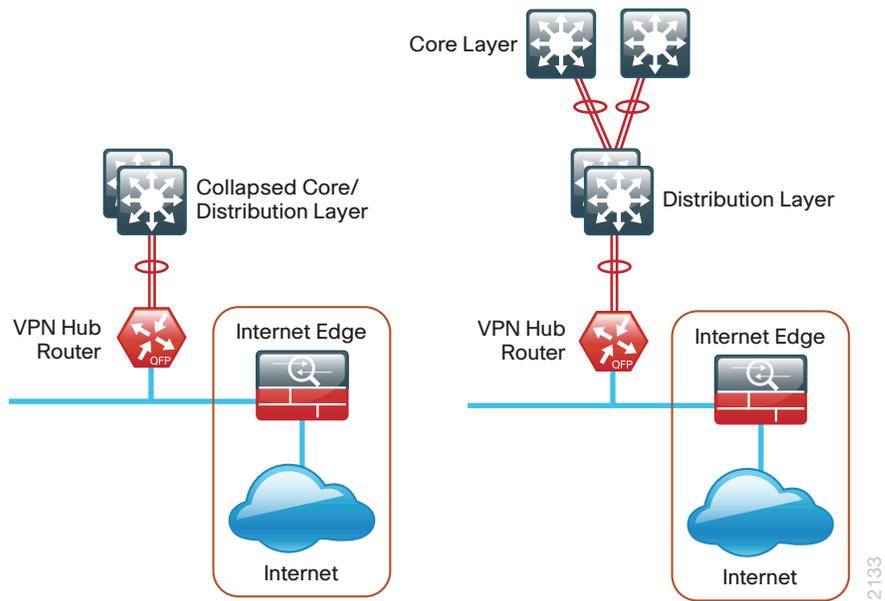
The characteristics of each design are discussed in the following sections.

### **DMVPN Only Design Model**

- Supports up to 100 remote sites
- Uses a single Internet link

The DMVPN Only design is shown in the following figure.

Figure 1 - DMVPN Only design model

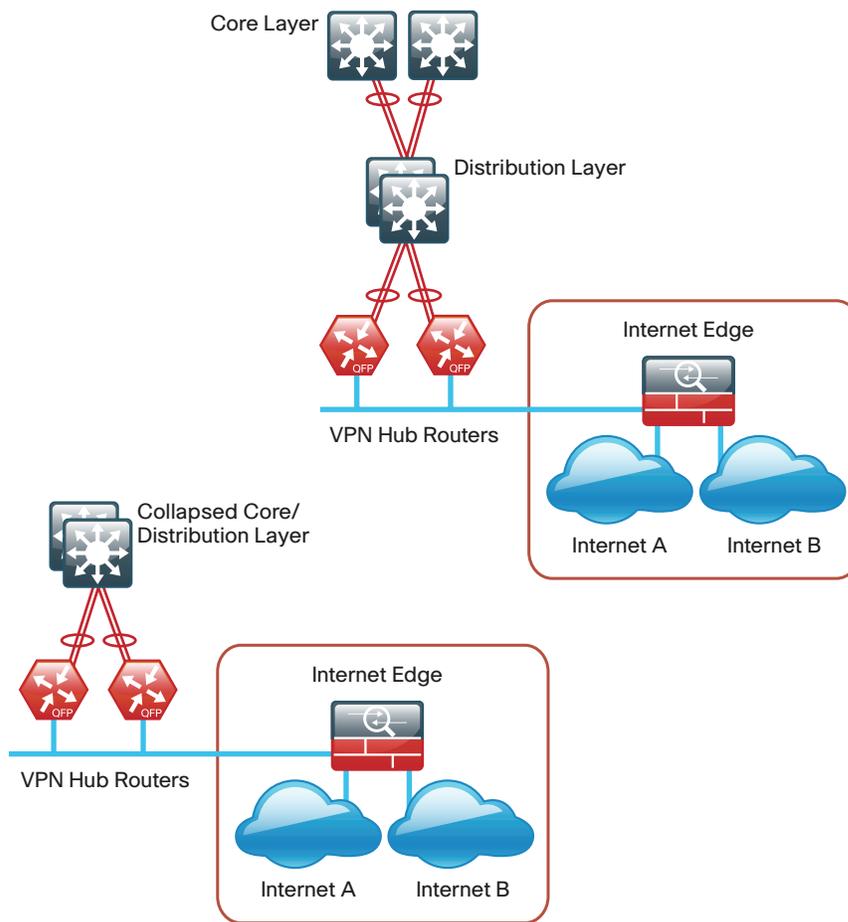


### Dual DMVPN Design Model

- Supports up to 500 remote sites
- Uses dual Internet links
- Typically used with a dedicated WAN distribution layer

The Dual DMVPN design is shown in the following figure.

Figure 2 - Dual DMVPN design model



2134

In both the DMVPN Only and Dual DMVPN design models, the DMVPN hub routers connect to the Internet indirectly through a firewall demilitarized zone (DMZ) interface contained within the Internet edge. For details about the connection to the Internet, see the [Firewall and IPS Technology Design Guide](#). The VPN hub routers are connected into the firewall DMZ interface, rather than connected directly with Internet service-provider routers.

### DMVPN Backup Shared Design Model

- Supports up to 50 remote sites
- Uses the same router for MPLS CE and VPN hub
- Has a single MPLS VPN carrier
- Uses static routing with MPLS VPN carrier
- Uses a single Internet link



The variants of the DMVPN Backup Dedicated design are shown in the following figures.

Figure 4 - DMVPN Backup Dedicated design model for MPLS WAN

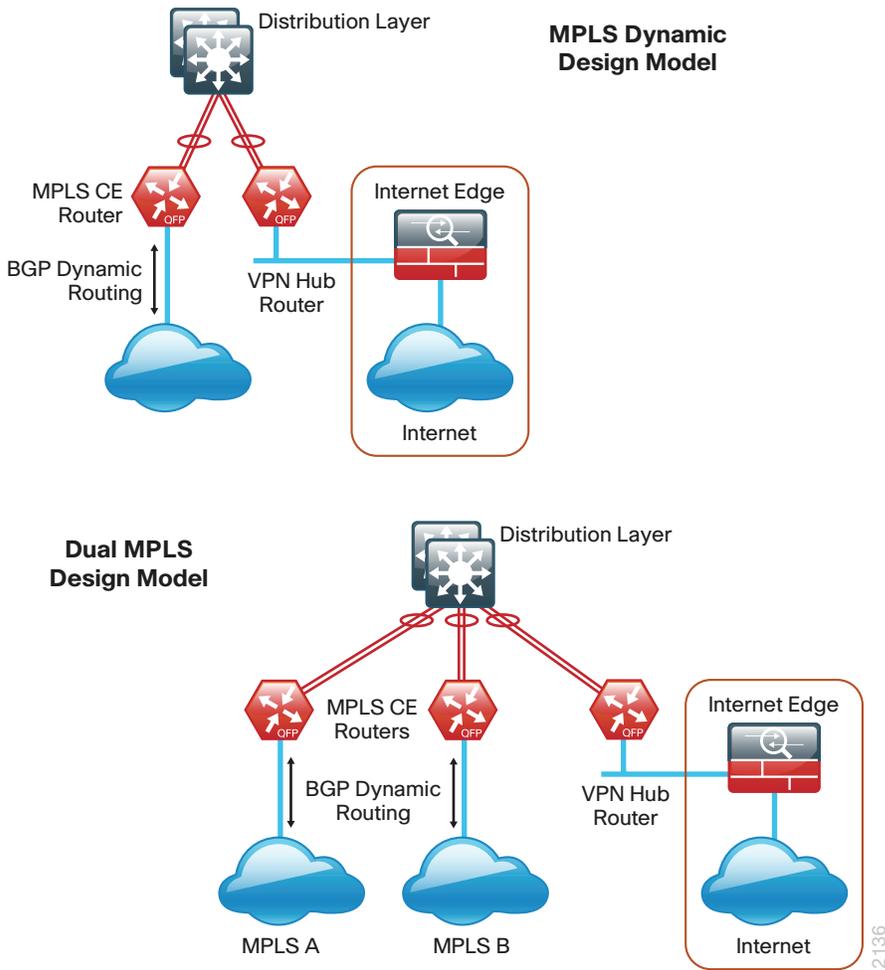
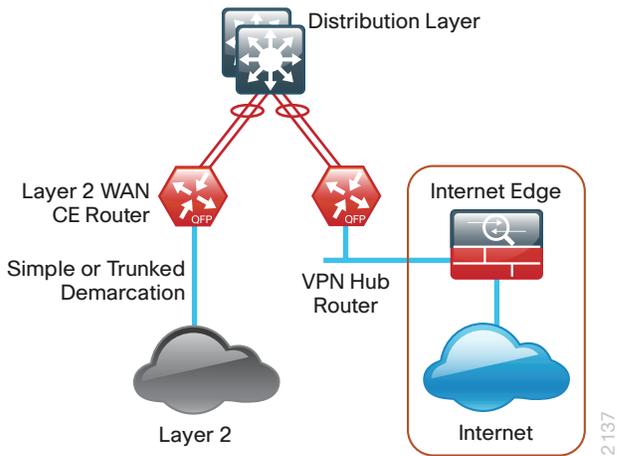


Figure 5 - DMVPN Backup Dedicated design model for Layer 2 WAN primary

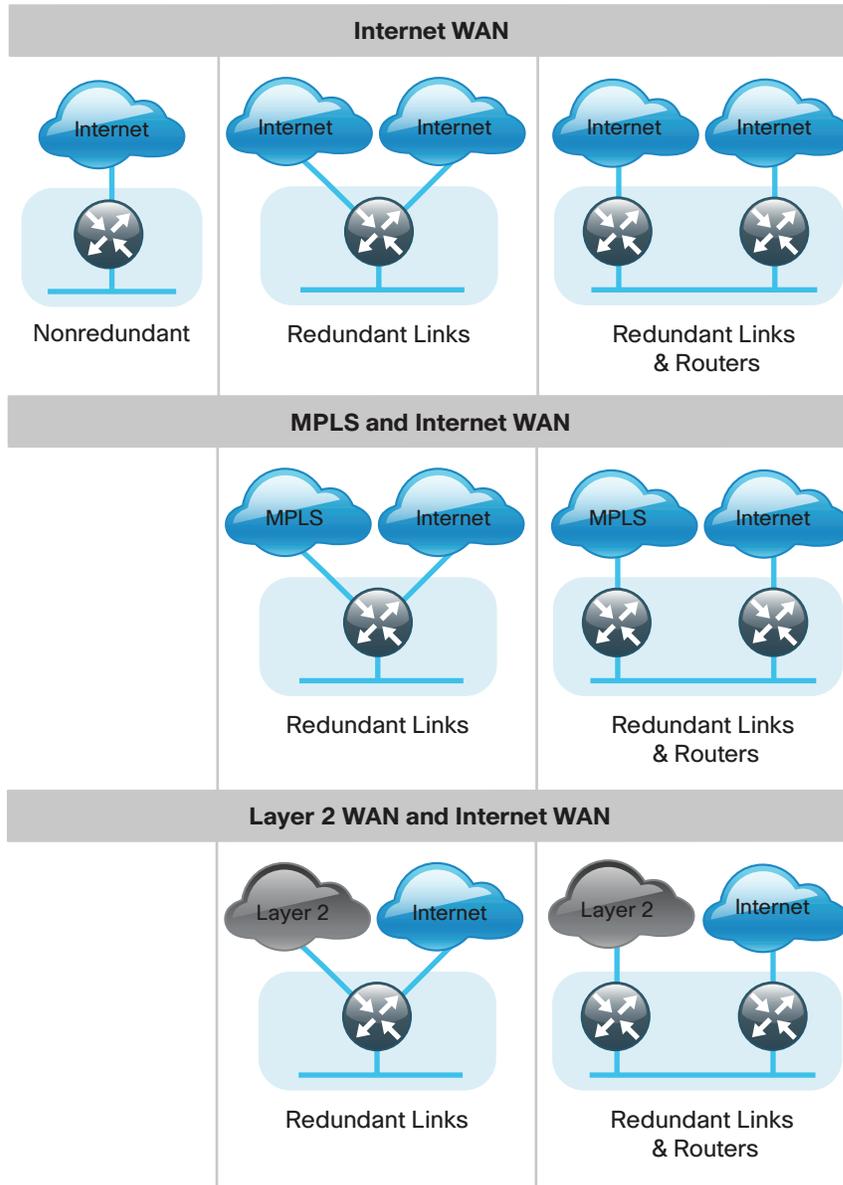


In the DMVPN Backup Dedicated design models, the DMVPN hub routers connect to the Internet indirectly through a firewall demilitarized zone (DMZ) interface contained within the Internet edge. For details about the connection to the Internet, see the [Firewall and IPS Technology Design Guide](#). The VPN hub routers are connected into the firewall DMZ interface, rather than connected directly with Internet service-provider routers.

### WAN Remote-Site Designs

This guide documents multiple WAN remote-site designs, and they are based on various combinations of WAN transports mapped to the site specific requirements for service levels and redundancy.

Figure 6 - WAN remote-site designs



2139

The remote-site designs include single or dual WAN edge routers. These can be either a CE router (for MPLS or Layer 2 WAN) or a VPN spoke router. In some cases, a single WAN edge router can perform the role of both a CE router and VPN spoke router.

Most remote sites are designed with a single router WAN edge; however, certain remote-site types require a dual router WAN edge. Dual router candidate sites include regional office or remote campus locations with large user populations, or sites with business critical needs that justify additional redundancy to remove single points of failure.

The overall WAN design methodology is based on a primary WAN-aggregation site design that can accommodate all of the remote-site types that map to the various link combinations listed in the following table.

Table 3 - WAN remote-site transport options

WAN remote- site routers	WAN transports	Primary transport	Secondary transport
Single	Single	Internet	–
Single	Dual	Internet	Internet
Dual	Dual	Internet	Internet
Single	Dual	MPLS VPN	Internet
Dual	Dual	MPLS VPN	Internet
Single	Dual	MetroE/VPLS	Internet
Dual	Dual	MetroE/VPLS	Internet

The modular nature of the network design enables you to create design elements that can be replicated throughout the network.

The WAN-aggregation designs and all of the WAN remote-site designs are standard building blocks in the overall design. Replication of the individual building blocks provides an easy way to scale the network and allows for a consistent deployment method.

### WAN/LAN Interconnection

The primary role of the WAN is to interconnect primary site and remote-site LANs. The LAN discussion within this guide is limited to how the WAN-aggregation site LAN connects to the WAN-aggregation devices and how the remote-site LANs connect to the remote-site WAN devices. Specific details regarding the LAN components of the design are covered in the [Campus Wired LAN Technology Design Guide](#).

At remote sites, the LAN topology depends on the number of connected users and physical geography of the site. Large sites may require the use of a distribution layer to support multiple access layer switches. Other sites may only require an access layer switch directly connected to the WAN remote-site routers. The variants that are tested and documented in this guide are shown in the following table.

Table 4 - WAN remote-site LAN options

WAN remote-site routers	WAN transports	LAN topology
Single	Single	Access only Distribution/Access
Single	Dual	Access only Distribution/Access
Dual	Dual	Access only Distribution/Access

## WAN Remotes Sites–LAN Topology

For consistency and modularity, all WAN remote sites use the same VLAN assignment scheme, which is shown in the following table. This design guide uses a convention that is relevant to any location that has a single access switch and this model can also be easily scaled to additional access closets through the addition of a distribution layer.

Table 5 - WAN remote-sites–VLAN assignment

VLAN	Usage	Layer 2 access	Layer 3 distribution/access
VLAN 64	Data 1	Yes	–
VLAN 69	Voice 1	Yes	–
VLAN 99	Transit	Yes (dual router only)	Yes (dual router only)
VLAN 50	Router Link (1)	–	Yes
VLAN 54	Router Link (2)	–	Yes (dual router only)

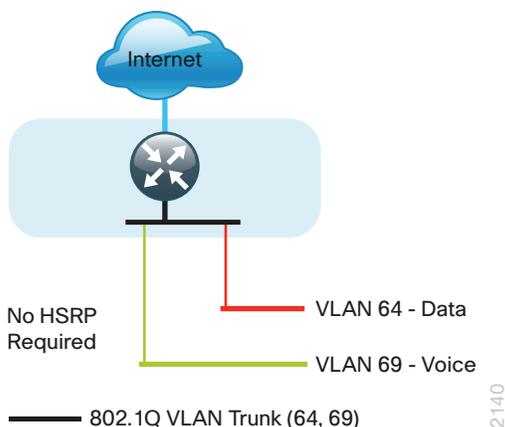
### Layer 2 Access

WAN remote sites that do not require additional distribution layer routing devices are considered to be flat or from a LAN perspective they are considered unrouted Layer 2 sites. All Layer 3 services are provided by the attached WAN routers. The access switches, through the use of multiple VLANs, can support services such as data and voice. The design shown in the following figure illustrates the standardized VLAN assignment scheme. The benefits of this design are clear: all of the access switches can be configured identically, regardless of the number of sites in this configuration.

Access switches and their configuration are not included in this guide. The [Campus Wired LAN Technology Design Guide](#) provides configuration details on the various access switching platforms.

IP subnets are assigned on a per-VLAN basis. This design only allocates subnets with a 255.255.255.0 netmask for the access layer, even if less than 254 IP addresses are required. (This model can be adjusted as necessary to other IP address schemes.) The connection between the router and the access switch must be configured for 802.1Q VLAN trunking with subinterfaces on the router that map to the respective VLANs on the switch. The various router subinterfaces act as the IP default gateways for each of the IP subnet and VLAN combinations.

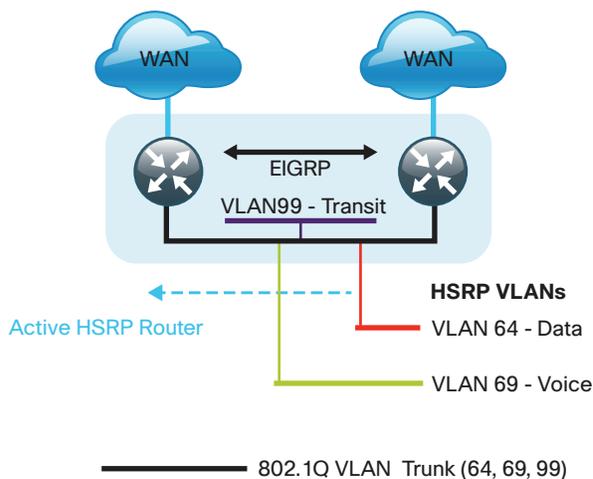
Figure 7 - WAN remote site–Flat Layer 2 LAN (single router)



A similar LAN design can be extended to a dual-router edge as shown in the following figure. This design change introduces some additional complexity. The first requirement is to run a routing protocol. You need to configure Enhanced Interior Gateway Protocol (EIGRP) between the routers. For consistency with the primary site LAN, use EIGRP process 100.

Because there are now two routers per subnet, a First Hop Redundancy Protocol (FHRP) must be implemented. For this design, Cisco selected Hot Standby Router Protocol (HSRP) as the FHRP. HSRP is designed to allow for transparent failover of the first-hop IP router. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active router and a standby router. When there are multiple routers on a LAN, the active router is the router of choice for routing packets; the standby router is the router that takes over when the active router fails or when preset conditions are met.

Figure 8 - WAN remote site—Flat Layer 2 LAN (dual router)



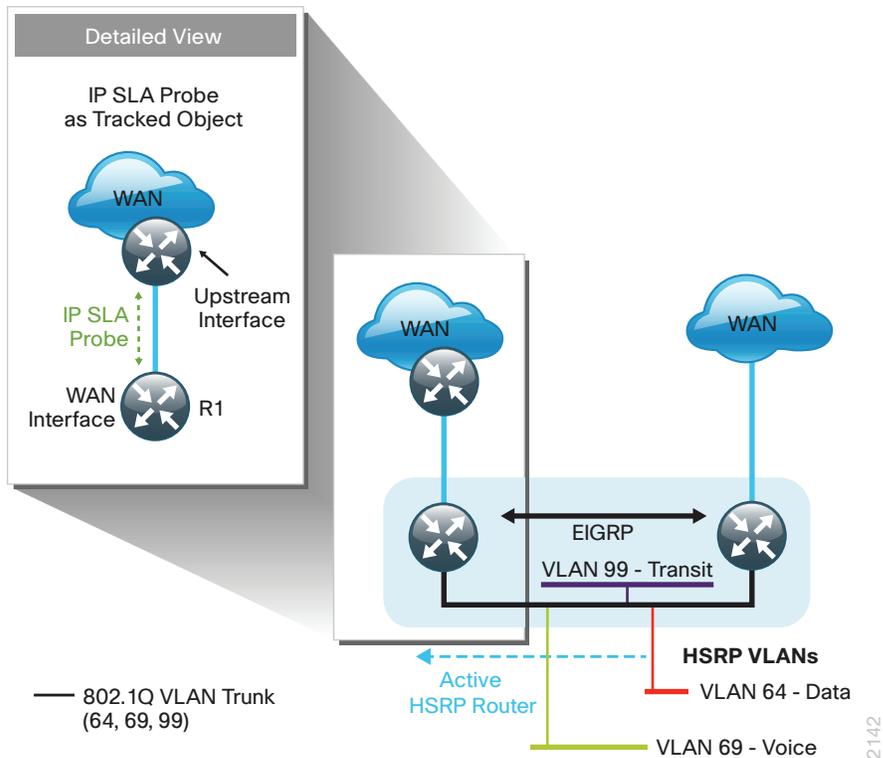
2141

Enhanced Object Tracking (EOT) provides a consistent methodology for various router and switching features to conditionally modify their operation based on information objects available within other processes. The objects that can be tracked include interface line protocol, IP route reachability, and IP service-level agreement (SLA) reachability as well as several others.

The IP SLA feature provides a capability for a router to generate synthetic network traffic that can be sent to a remote responder. The responder can be a generic IP endpoint that can respond to an Internet Control Message Protocol (ICMP) echo (ping) request, or can be a Cisco router running an IP SLA responder process, that can respond to more complex traffic such as jitter probes. The use of IP SLA allows the router to determine end-to-end reachability to a destination and also the roundtrip delay. More complex probe types can also permit the calculation of loss and jitter along the path. IP SLA is used in tandem with EOT within this design.

To improve convergence times after a primary WAN failure, HSRP has the capability to monitor the reachability of a next-hop IP neighbor through the use of EOT and IP SLA. This combination allows for a router to give up its HSRP Active role if its upstream neighbor becomes unresponsive and that provides additional network resiliency.

Figure 9 - WAN remote-site-IP SLA probe to verify upstream device reachability



HSRP is configured to be active on the router with the highest priority WAN transport. EOT of IP SLA probes is implemented in conjunction with HSRP so that in the case of WAN transport failure, the standby HSRP router associated with the lower priority (alternate) WAN transport becomes the active HSRP router. The IP SLA probes are sent from the remote-site primary WAN router to the upstream neighbor (MPLS PE, Layer 2 WAN CE, or DMVPN hub) to ensure reachability of the next hop router. This is more effective than simply monitoring the status of the WAN interface.

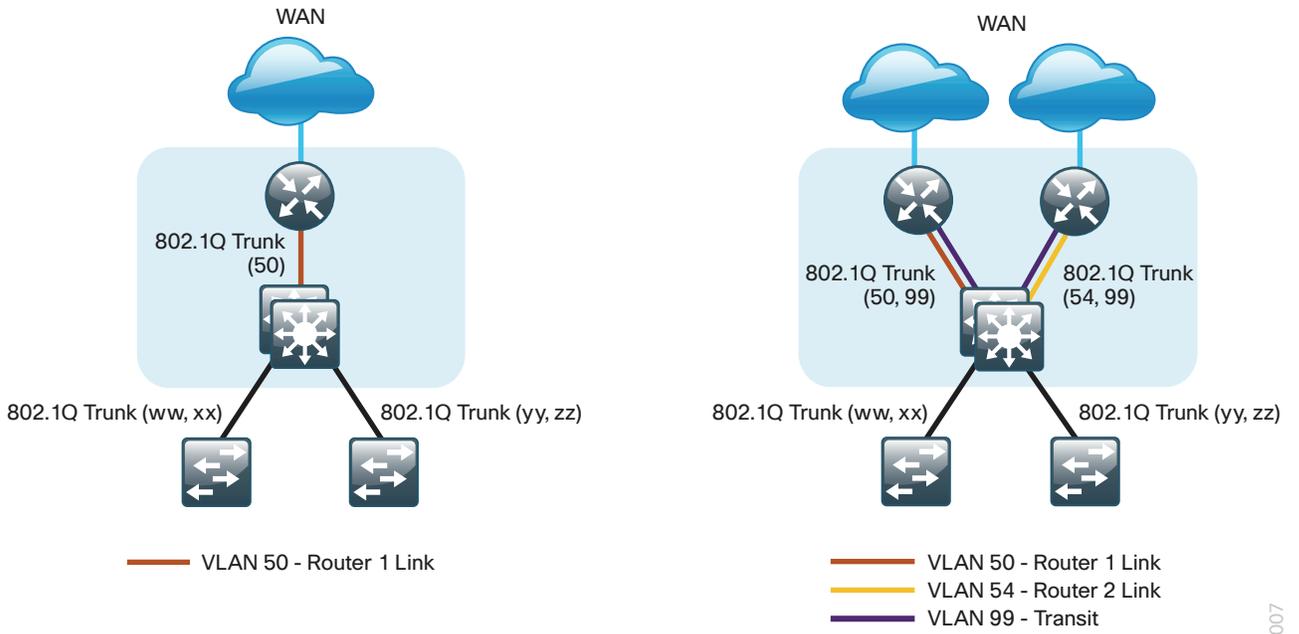
The dual router designs also warrant an additional component that is required for proper routing in certain scenarios. In these cases, a traffic flow from a remote-site host might be sent to a destination reachable via the alternate WAN transport (for example, a dual DMVPN remote site communicating with a DMVPN2-only remote site). The primary WAN transport router then forwards the traffic out the same data interface to send it to the alternate WAN transport router, which then forwards the traffic to the proper destination. This is referred to as hairpinning.

The appropriate method to avoid sending the traffic out the same interface is to introduce an additional link between the routers and designate the link as a transit network (Vlan 99). There are no hosts connected to the transit network, and it is only used for router-router communication. The routing protocol runs between router subinterfaces assigned to the transit network. No additional router interfaces are required with this design modification because the 802.1Q VLAN trunk configuration can easily accommodate an additional subinterface.

### Distribution and Access Layer

Large remote sites may require a LAN environment similar to that of a small campus LAN that includes a distribution layer and access layer. This topology works well with either a single or dual router WAN edge. To implement this design, the routers should connect via EtherChannel links to the distribution switch. These EtherChannel links are configured as 802.1Q VLAN trunks, to support both a routed point-to-point link to allow EIGRP routing with the distribution switch, and in the dual router design, to provide a transit network for direct communication between the WAN routers.

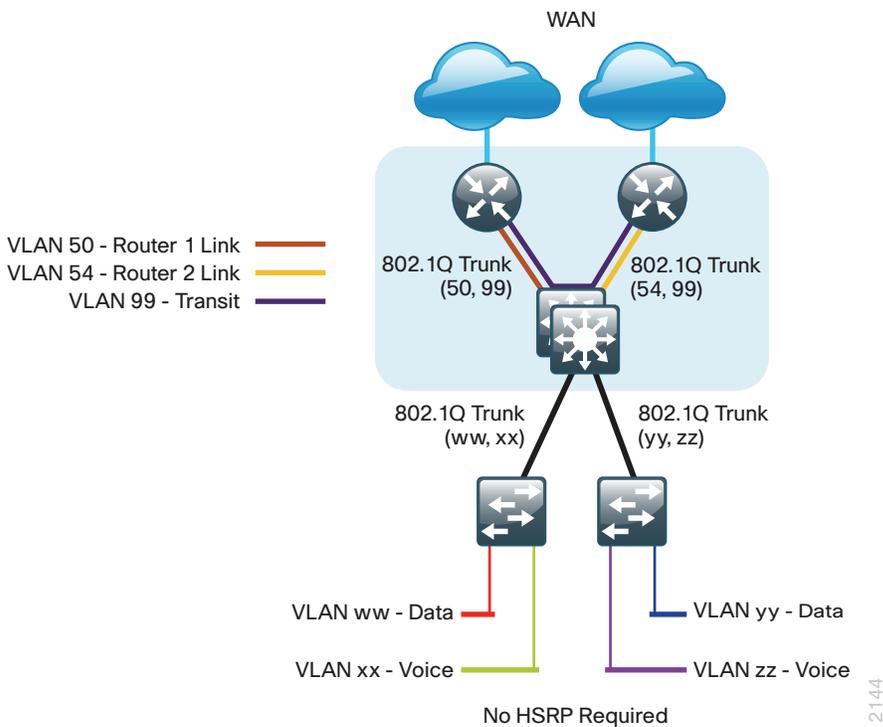
Figure 10 - WAN remote-site-Connection to distribution layer



2007

The distribution switch handles all access layer routing, with VLANs trunked to access switches. No HSRP is required when the design includes a distribution layer. A full distribution and access layer design is shown in the following figure.

Figure 11 - WAN remote-site-Distribution and access layer (dual router)



2144

## IP Multicast

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. IP Multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP telephony Music On Hold (MOH) and IP video broadcast streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an Internet Group Management Protocol (IGMP) message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as a rendezvous point (RP) to map the receivers to active sources so that they can join their streams.

The RP is a control-plane operation that should be placed in the core of the network or close to the IP Multicast sources on a pair of Layer 3 switches or routers. IP Multicast routing begins at the distribution layer if the access layer is Layer 2 and provides connectivity to the IP Multicast RP. In designs without a core layer, the distribution layer performs the RP function.

This design is fully enabled for a single global scope deployment of IP Multicast. The design uses an Anycast RP implementation strategy. This strategy provides load sharing and redundancy in Protocol Independent Multicast sparse mode (PIM SM) networks. Two RPs share the load for source registration and the ability to act as hot backup routers for each other.

The benefit of this strategy from the WAN perspective is that all IP routing devices within the WAN use an identical configuration referencing the Anycast RPs. IP PIM SM is enabled on all interfaces including loopbacks, VLANs and subinterfaces.

## Quality of Service

Most users perceive the network as just a transport utility mechanism to shift data from point A to point B as fast as it can. Many sum this up as just “speeds and feeds.” While it is true that IP networks forward traffic on a best-effort basis by default, this type of routing only works well for applications that adapt gracefully to variations in latency, jitter, and loss. However networks are multiservice by design and support real-time voice and video as well as data traffic. The difference is that real-time applications require packets to be delivered within specified loss, delay, and jitter parameters.

In reality, the network affects all traffic flows and must be aware of end-user requirements and services being offered. Even with unlimited bandwidth, time-sensitive applications are affected by jitter, delay, and packet loss. Quality of Service (QoS) enables a multitude of user services and applications to coexist on the same network.

Within the architecture, there are wired and wireless connectivity options that provide advanced classification, prioritizing, queuing, and congestion mechanisms as part of the integrated QoS to help ensure optimal use of network resources. This functionality allows for the differentiation of applications, ensuring that each has the appropriate share of the network resources to protect the user experience and ensure the consistent operations of business critical applications.

QoS is an essential function of the network infrastructure devices used throughout this architecture. QoS enables a multitude of user services and applications, including real-time voice, high-quality video, and delay-sensitive data to coexist on the same network. In order for the network to provide predictable, measurable, and sometimes guaranteed services, it must manage bandwidth, delay, jitter, and loss parameters. Even if you do not require QoS for your current applications, you can use QoS for management and network protocols to protect the network functionality and manageability under normal and congested traffic conditions.

The goal of this design is to provide sufficient classes of service to allow you to add voice, interactive video, critical data applications, and management traffic to the network, either during the initial deployment or later with minimum system impact and engineering effort.

The QoS classifications in the following table are applied throughout this design. This table is included as a reference.

Table 6 - QoS service class mappings

<b>Service class</b>	<b>Per-hop-behavior (PHB)</b>	<b>Differentiated services code point (DSCP)</b>	<b>IP Precedence(IPP)</b>	<b>Class of service (CoS)</b>
Network layer	Layer 3	Layer 3	Layer 3	Layer 2
Network control	CS6	48	6	6
Telephony	EF	46	5	5
Signaling	CS3	24	3	3
Multimedia conferencing	AF41, 42, 43	34, 36, 38	4	4
Real-Time interactive	CS4	32	4	4
Multimedia streaming	AF31, 32, 33	26, 28, 30	3	3
Broadcast video	CS5	40	4	4
Low-latency data	AF21, 22, 23	18, 20, 22	2	2
Operation, administration, and maintenance (OAM)	CS2	16	2	2
Bulk data	AF11, 12, 13	10, 12, 14	1	1
Scavenger	CS1	8	1	1
Default "best effort"	DF	0	0	0

# Deploying the WAN

## Overall WAN Architecture Design Goals

### IP Routing

The design has the following IP routing goals:

- Provide optimal routing connectivity from primary WAN-aggregation sites to all remote locations
- Isolate WAN routing topology changes from other portions of the network
- Ensure active/standby symmetric routing when multiple paths exist, for ease of troubleshooting and to prevent oversubscription of IP telephony Call Admission Control (CAC) limits
- Provide site-site remote routing via the primary WAN-aggregation site (hub-and-spoke model)
- Permit optimal direct site-site remote routing when carrier services allow (spoke-to-spoke model)
- Support IP Multicast sourced from the primary WAN-aggregation site

At the WAN remote sites, there is no local Internet access for web browsing or cloud services. This model is referred to as a centralized Internet model. It is worth noting that sites with Internet/DMVPN for either primary or backup transport could potentially provide local Internet capability; however, for this design, only encrypted traffic to other DMVPN sites is permitted to use the Internet link. In the centralized Internet model, a default route is advertised to the WAN remote sites in addition to the internal routes from the data center and campus.

### LAN Access

All remote sites are to support both wired LAN access.

### High Availability

The network must tolerate single failure conditions including the failure of any single WAN transport link or any single network device at the primary WAN-aggregation site.

- Remote sites classified as single-router, dual-link must be able to tolerate the loss of either WAN transport.
- Remote sites classified as dual-router, dual-link must be able to tolerate the loss of either an edge router or a WAN transport.

### Path Selection Preferences

There are many potential traffic flows based on which WAN transports are in use and whether or not a remote site is using a dual WAN transport.

The single WAN transport routing functions as follows.

DMVPN-connected site:

- Connects to a site on the same DMVPN; the optimal route is direct within the DMVPN (only initial traffic is sent to the DMVPN hub, and then is cut-through via spoke-spoke tunnel).
- Connects to any other site; the route is through the primary site.

The use of the dual WAN transports is specifically tuned where possible to behave in an active/standby manner. This type of configuration provides symmetric routing, with traffic flowing along the same path in both directions. Symmetric routing simplifies troubleshooting because bidirectional traffic flows always traverse the same links.

Each design assumes that one of the WAN transports is designated as the primary transport, which is the preferred path in most conditions.

DMVPN (primary) + DMVPN (secondary) dual-connected site:

- Connects to a site on the same DMVPN; the optimal route is direct within the DMVPN (only initial traffic is sent to the DMVPN hub, and then is cut-through via spoke-spoke tunnel).
- Connects to any other site; the route is through the primary site.

MPLS VPN (primary) + DMVPN (secondary) dual-connected site:

- Connects to a site on the same MPLS VPN; the optimal route is direct within the MPLS VPN (traffic is not sent to the primary site).
- Connects to any DMVPN single-connected site; the optimal route is direct within the DMVPN (only initial traffic is sent to the DMVPN hub, and then is cut through via spoke-spoke tunnel).
- Connects to any other site; the route is through the primary site

Layer 2 WAN (primary) + DMVPN (secondary) dual-connected site:

- Connects to a site on the Layer 2 WAN (same VLAN); the optimal route is direct within the Layer 2 WAN (traffic is not sent to the primary site).
- Connects to any DMVPN single-connected site; the optimal route is direct within the DMVPN (only initial traffic is sent to the DMVPN hub, and then it is cut through via spoke-spoke tunnel).
- Connects to any other site; the route is through the primary site

## Data Privacy (Encryption)

All remote-site traffic must be encrypted when transported over public IP networks such as the Internet.

The use of encryption should not limit the performance or availability of a remote-site application, and should be transparent to end users.

## Quality of Service (QoS)

The network must ensure that business applications perform across the WAN during times of network congestion. Traffic must be classified and queued and the WAN connection must be shaped to operate within the capabilities of the connection. When the WAN design uses a service provider offering with QoS, the WAN edge QoS classification and treatment must align to the service provider offering to ensure consistent end-to-end QoS treatment of traffic.

## Design Parameters

This design guide uses certain standard design parameters and references various network infrastructure services that are not located within the WAN. These parameters are listed in the following table.

*Table 7 - Universal design parameters*

Network service	IP address
Domain name	cisco.local
Active Directory, DNS server, DHCP server	10.4.48.10
Cisco Secure Access Control System (ACS)	10.4.48.15
Network Time Protocol (NTP) server	10.4.48.17

# Deploying a DMVPN WAN

## Design Overview

### DMVPN Hub Routers

The DMVPN designs are intended to support up to 500 remote sites with a combined aggregate WAN bandwidth of up to 1.0 Gbps. The most critical devices are the WAN routers that are responsible for reliable IP forwarding and QoS. The amount of bandwidth required at the WAN-aggregation site determines which model of router to use. The choice of whether to implement a single router or dual router is determined by the number of DMVPN clouds that are required in order to provide connections to all of the remote sites.

Cisco ASR 1000 Series Aggregation Services Routers represent the next-generation, modular, services-integrated Cisco routing platform. They are specifically designed for WAN aggregation, with the flexibility to support a wide range of 3- to 16-mpps (millions of packets per second) packet-forwarding capabilities, 2.5- to 40-Gbps system bandwidth performance, and scaling.

The Cisco ASR 1000 Series is fully modular from both hardware and software perspectives, and the routers have all the elements of a true carrier-class routing product that serves both enterprise and service-provider networks.

This design uses the following routers as DMVPN hub routers:

- Cisco ASR 1002-X router configured with an embedded services processor (ESP) default bandwidth of 5 Gbps upgradable with software licensing options to 10 Gbps, 20 Gbps and 36 Gbps.
- Cisco ASR 1002 router configured with an embedded services processor 5 (ESP5)
- Cisco ASR 1001 router fixed configuration with a 2.5 Gbps embedded services processor
- Cisco 3945 Integrated Services Router
- Cisco 3925 Integrated Services Router

All of the design models can be constructed using any of the DMVPN hub routers listed in Table 8. You should consider the following: the forwarding performance of the router using an Ethernet WAN deployment with broad services enabled, the router's alignment with the suggested design model, and the number of remote sites.

Table 8 - DMVPN hub router options

Option	Cisco 3925	Cisco 3945	ASR 1001	ASR 1002	ASR 1002-X
Ethernet WAN with services	100 Mbps	150 Mbps	250 Mbps	500 Mbps	500 Mbps - 1.5 Gbps
Software Redundancy Option	None	None	Yes	Yes	Yes
Redundant power supply	Option	Option	Default	Default	Default
Supported Design Models	All	All	All	All	All
Suggested Design Model (s)	DMVPN Backup Shared	DMVPN Backup Shared	DMVPN Only DMVPN Backup Dedicated	Dual DMVPN DMVPN Backup Dedicated	Dual DMVPN DMVPN Backup Dedicated
Suggested Number of Remote Sites	25	50	100	250	250+

## Remote Sites–DMVPN Spoke Router Selection

The actual WAN remote-site routing platforms remain unspecified because the specification is tied closely to the bandwidth required for a location and the potential requirement for the use of service module slots. The ability to implement this solution with a variety of potential router choices is one of the benefits of a modular design approach.

There are many factors to consider in the selection of the WAN remote-site routers. Among those, and key to the initial deployment, is the ability to process the expected amount and type of traffic. You also need to make sure that you have enough interfaces, enough module slots, and a properly licensed Cisco IOS Software image that supports the set of features that is required by the topology. Cisco tested multiple integrated service router models as DMVPN spoke routers, and the expected performance is shown in the following table.

Table 9 - WAN remote-site Cisco Integrated Service Router options

Option	1941 <sup>1</sup>	2911	2921	2951	3925	3945	4451-X
Ethernet WAN with Services <sup>2</sup>	25 Mbps	35 Mbps	50 Mbps	75 Mbps	100 Mbps	150 Mbps	1 Gbps
On-board GE ports <sup>3</sup>	2	3	3	3	3	3	4
Service module slots <sup>4</sup>	0	1	1	2	2	4	2
Redundant power supply option	No	No	No	No	Yes	Yes	Yes

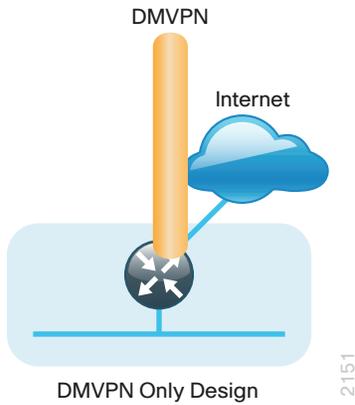
### Notes:

1. The Cisco 1941 Integrated Services Router is recommended for use at single-router, single-link remote sites.
2. The performance numbers are conservative numbers obtained when the router is passing IMIX traffic with heavy services configured and the CPU utilization is under 75 percent.
3. A single-router, dual-link remote-site requires 4 router interfaces when using a port-channel to connect to an access or distribution layer. Add the EHWIC-1GE-SFP-CU to the Cisco 2900 and 3900 Series Integrated Services Routers in order to provide the additional WAN-facing interface.
4. Not all service modules are supported in Cisco 4451-X ISR. Some service modules are double-wide.

The DMVPN spoke routers at the WAN remote sites connect to the Internet directly through a router interface. More details about the security configuration of the remote-site routers connected to the Internet are discussed later in this guide. The single link DMVPN remote site is the most basic of building blocks for any remote location. This design can be used with the DMVPN spoke router connected directly to the access layer, or it can support a more complex LAN topology by connecting the DMVPN spoke router directly to a distribution layer.

The IP routing is straightforward and can be handled entirely by static routes at the WAN-aggregation site and static default routes at the remote site. However, there is significant value to configuring this type of site with dynamic routing. It is easy to add or modify IP networks at the remote site when using dynamic routing because any changes are immediately propagated to the rest of the network.

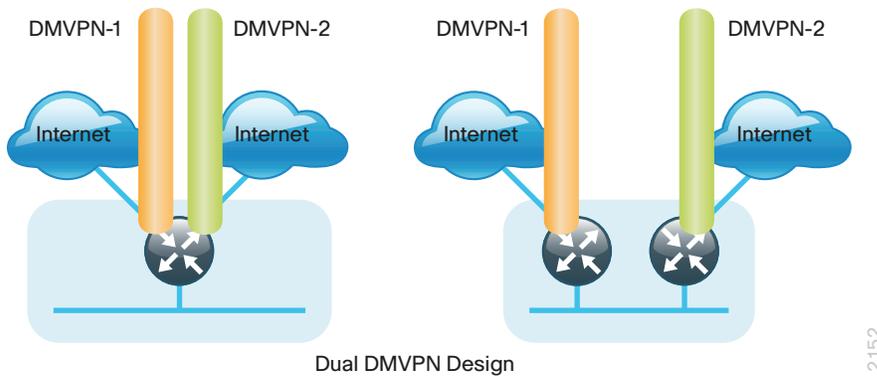
Figure 12 - DMVPN remote site (single link–single router)



The DMVPN connection can be the primary WAN transport, or it can also be the alternate to another DMVPN WAN transport. A DMVPN backup link can be added to an existing DMVPN single-link design to provide additional resiliency either connecting on the same router or on an additional router. By adding an additional link, you provide the first level of high availability for the remote site. A failure in the primary link can be automatically detected by the router and traffic can be rerouted to the secondary path. It is mandatory to run dynamic routing when there are multiple paths. The routing protocols are tuned to ensure the proper path selection.

The dual-router, dual-link design continues to improve upon the level of high availability for the site. This design can tolerate the loss of the primary router and traffic can be rerouted via the secondary router (through the alternate path).

Figure 13 - DMVPN + DMVPN remote site (dual link options)



The DMVPN connection can also be the alternate to an existing MPLS WAN or Layer 2 WAN transport. You can add a DMVPN backup link to either a MPLS WAN or Layer 2 WAN single-link design to provide additional resiliency by either connecting on the same router or on an additional router. The same resiliency benefits of the DMVPN dual-link options apply to the MPLS + DMVPN and Layer 2 + DMVPN options. The single-router and dual-router options are shown respectively in Figure 14 and Figure 15.

Figure 14 - MPLS + DMVPN and Layer 2 WAN + DMVPN remote site (single-router, dual link)

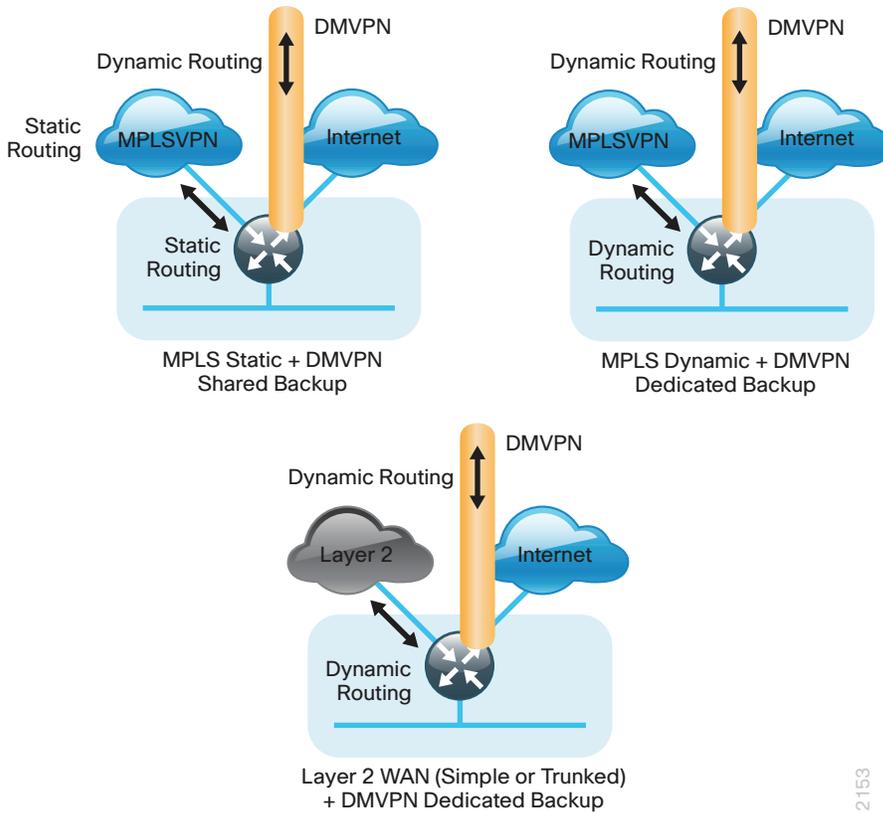
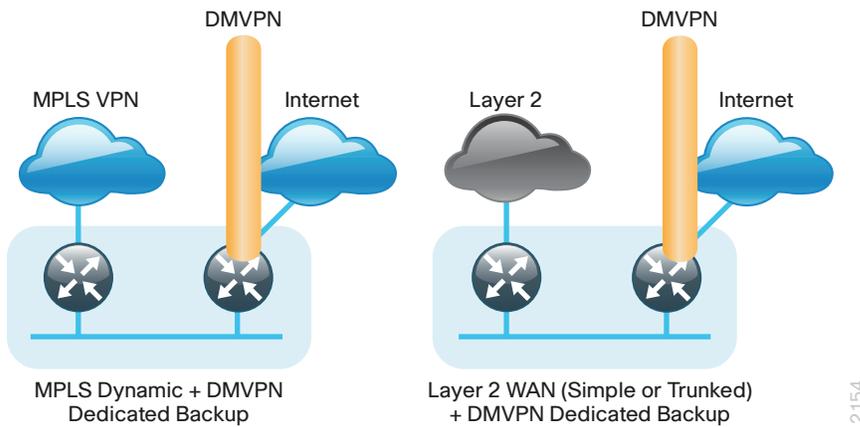


Figure 15 - MPLS + DMVPN and Layer 2 WAN + DMVPN remote site (dual-router, dual link)



## VRFs and Front Door VRF

Virtual Route Forwarding (VRF) is a technology used in computer networks that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, you can use the same or overlapping IP Addresses without conflicting with each other. Often in a MPLS context, VRF is also defined as VPN Route Forwarding.

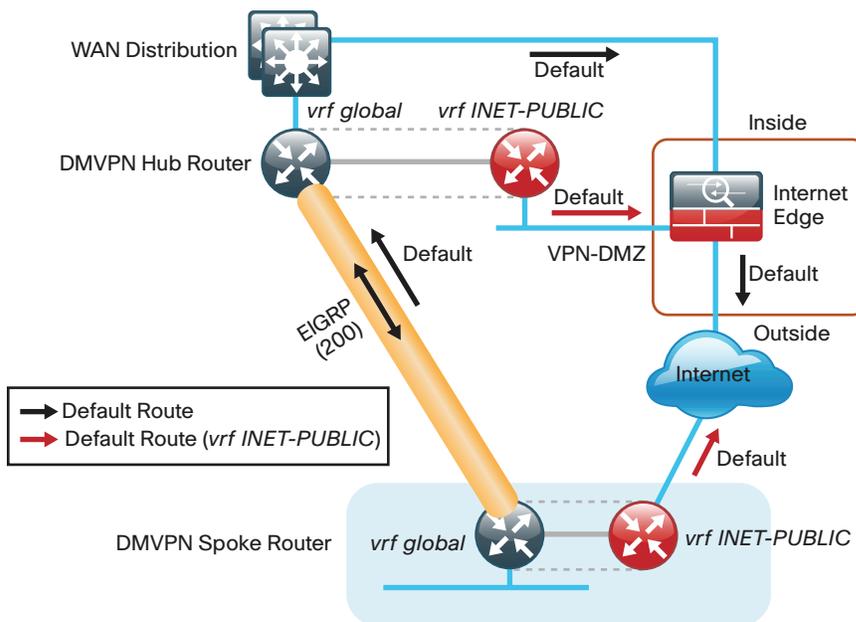
You can implement VRF in a network device by having distinct routing tables, also known as Forwarding Information Bases (FIBs), one per VRF. Alternatively, a network device may have the ability to configure different virtual routers, where each one has its own FIB that is not accessible to any other virtual router instance on the same device.

The simplest form of VRF implementation is VRF Lite. In this implementation, each router within the network participates in the virtual routing environment on a peer-by-peer basis. VRF Lite configurations are only locally significant.

The IP routing policy used in this design for the WAN remote sites does not allow direct Internet access for web browsing or other uses; any remote-site hosts that access the Internet must do so via the Internet edge at the primary site. The end hosts require a default route for all Internet destinations; however, this route must force traffic across the primary or secondary WAN transport DMVPN tunnels. This requirement conflicts with the more general VPN spoke router requirement for an Internet-facing default route to bring up the VPN tunnel.

The multiple default route conundrum is solved through the use of VRFs on the router. A router can have multiple routing tables that are kept logically separate on the device. This separation is similar to a virtual router from the forwarding plane perspective. The global VRF corresponds to the traditional routing table, and additional VRFs are given names and route descriptors (RDs). Certain features on the router are VRF aware, including static routing and routing protocols, interface forwarding and IPsec tunneling. This set of features is used in conjunction with DMVPN to permit the use of multiple default routes for both the DMVPN hub routers and DMVPN spoke routers. This combination of features is referred to as front-door vREF (FVRF), because the VRF faces the Internet and the router internal interfaces and the mGRE tunnel all remain in the global VRF. More technical details regarding FVRF can be found in the Technical Feature Supplement appendix.

Figure 16 - Front door VRF (FVRF)



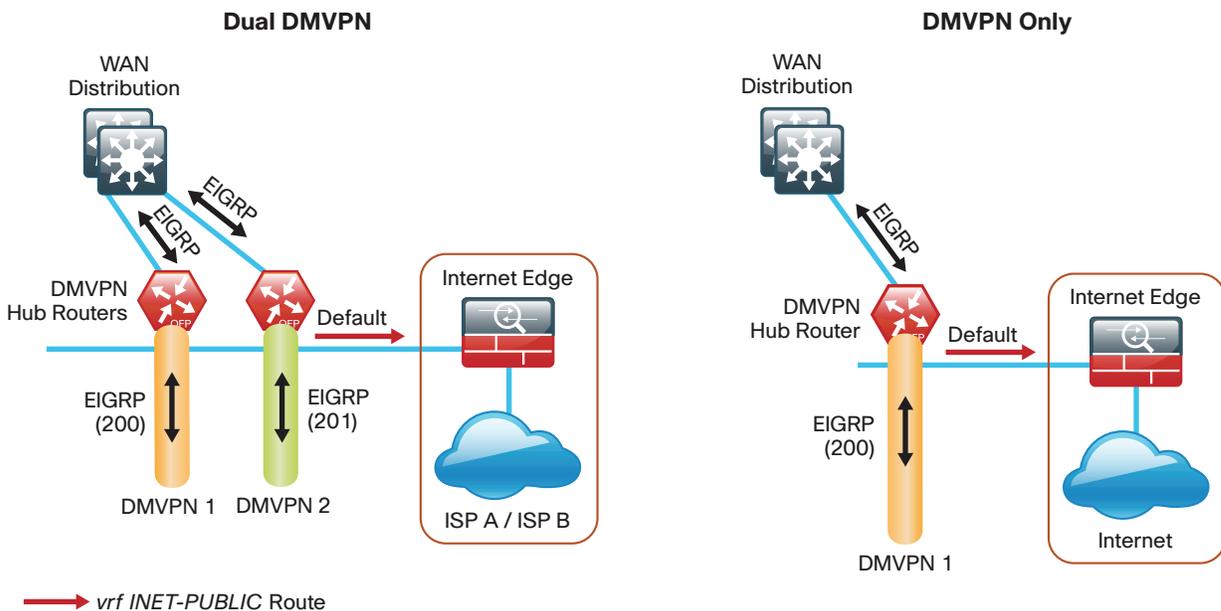
## Design Details

The DMVPN hub routers connect to a resilient switching device in the distribution layer and in the DMZ. The DMVPN routers use EtherChannel connections consisting of two port bundles. This design provides both resiliency and additional forwarding performance. Additional forwarding performance can be accomplished by increasing the number of physical links within an EtherChannel.

The DMVPN hub routers must have sufficient IP-routing information to provide end-to-end reachability. Maintaining this routing information typically requires a routing protocol, EIGRP is used for this purpose. Multiple separate EIGRP processes are used, one for internal routing on the LAN (EIGRP-100) and multiple for the DMVPNs (EIGRP-200, EIGRP-201). The primary reason for the separate EIGRP processes is to ensure compatibility with the route selection process at the WAN-aggregation site when deploying other CVD WAN designs. This method ensures DMVPN learned routes appear as EIGRP external routes after they are redistributed into the EIGRP-100 process used on the campus LAN.

At the WAN-aggregation site, you must connect the DMVPN routers to the distribution layer and to the DMZ-VPN that provides Internet connectivity. The DMVPN hub routers use FVRF and have a static default route with the INET-PUBLIC VRF pointing to the firewall DMZ interface.

Figure 17 - Dual DMVPN and DMVPN Only designs—Routing details



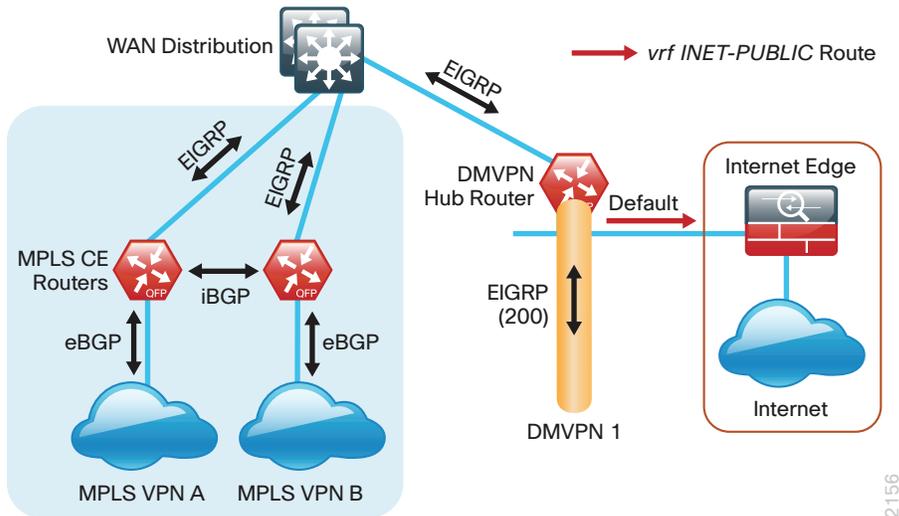
2155

The DMVPN Backup Dedicated Design Model is essentially the DMVPN Only or Dual DMVPN design models merged with any of the following already deployed design models from the [MPLS WAN Technology Design Guide](#) or the [Layer 2 WAN Technology Design Guide](#):

- MPLS Dynamic
- Dual MPLS
- Layer 2 WAN Simple Demarcation
- Layer 2 WAN Trunked Demarcation

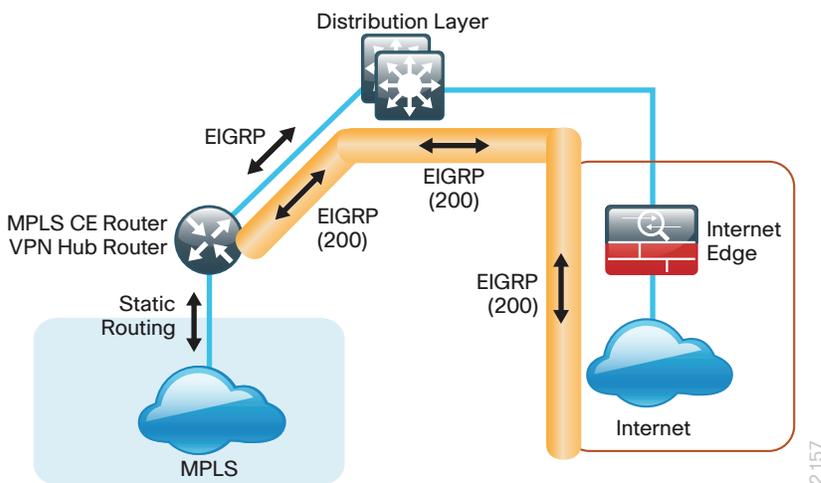
An example of the routing details for the DMVPN Backup Dedicated design model is shown in the following figure.

Figure 18 - DMVPN Backup Dedicated design—Routing details



The DMVPN Shared Backup design does not require any additional hardware. The existing MPLS Static design from the [MPLS WAN Technology Design Guide](#) already includes a WAN-aggregation MPLS CE router and Internet access. The primary difference is the VPN connection and the requirement to run a routing protocol for the VPN backup link. The MPLS WAN connection continues to use static routing in these designs. The routing details are shown for these designs are shown in the following figure.

Figure 19 - DMVPN Shared Backup design—Routing details



## EIGRP

Cisco uses Enhanced IGRP (EIGRP) as the primary routing protocol because it is easy to configure, does not require a large amount of planning, has flexible summarization and filtering, and can scale to large networks. As networks grow, the number of IP prefixes or routes in the routing tables grows as well. You should program IP summarization on links where logical boundaries exist, like distribution layer links to the wide area or to a core. By performing IP summarization, you can reduce the amount of bandwidth, processor, and memory necessary to carry large route tables, and reduce convergence time associated with a link failure.

In this design, EIGRP process 100 is the primary EIGRP process and is referred to as EIGRP-100.

EIGRP-100 is used at the WAN-aggregation site to connect to the primary site LAN distribution layer and at WAN remote sites with dual WAN routers or with distribution-layer LAN topologies. EIGRP-200 and EIGRP-201 are used for the DMVPN tunnels.

## Encryption

The primary goal of encryption is to provide data confidentiality, integrity, and authenticity by encrypting IP packets as the data travels across a network.

The encrypted payloads are then encapsulated with a new header (or multiple headers) and transmitted across the network. The additional headers introduce a certain amount of overhead to the overall packet length. The following table highlights the packet overhead associated with encryption based on the additional headers required for various combinations of IPsec and GRE.

Table 10 - Overhead associated with IPsec and GRE

Encapsulation	Overhead
GRE only	24 bytes
IPsec (Transport Mode)	36 bytes
IPsec (Tunnel Mode)	52 bytes
IPsec (Transport Mode) + GRE	60 bytes
IPsec (Tunnel Mode) + GRE	76 bytes

There is a maximum transmission unit (MTU) parameter for every link in an IP network and typically the MTU is 1500 bytes. IP packets larger than 1500 bytes must be fragmented when transmitted across these links. Fragmentation is not desirable and can impact network performance. To avoid fragmentation, the original packet size plus overhead must be 1500 bytes or less, which means that the sender must reduce the original packet size. To account for other potential overhead, Cisco recommends that you configure tunnel interfaces with a 1400 byte MTU.

There are dynamic methods for network clients to discover the path MTU, which allow the clients to reduce the size of packets they transmit. However, in many cases, these dynamic methods are unsuccessful, typically because security devices filter the necessary discovery traffic. This failure to discover the path MTU drives the need for a method that can reliably inform network clients of the appropriate packet size. The solution is to implement the **ip tcp adjust mss [size]** command on the WAN routers, which influences the TCP maximum segment size (MSS) value reported by end hosts.

The MSS defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.

The IP and TCP headers combine for 40 bytes of overhead, so the typical MSS value reported by network clients will be 1460. This design includes encrypted tunnels with a 1400 byte MTU, so the MSS used by endpoints should be configured to be 1360 to minimize any impact of fragmentation. In this solution, you implement the **ip tcp adjust mss 1360** command on all WAN facing router interfaces.

## DMVPN

This solution uses the Internet for WAN transport. For data security and privacy concerns any site-to-site traffic that traverses the Internet must be encrypted. Multiple technologies can provide encryption, but the method that provides the best combination of performance, scale, application support, and ease of deployment is DMVPN.

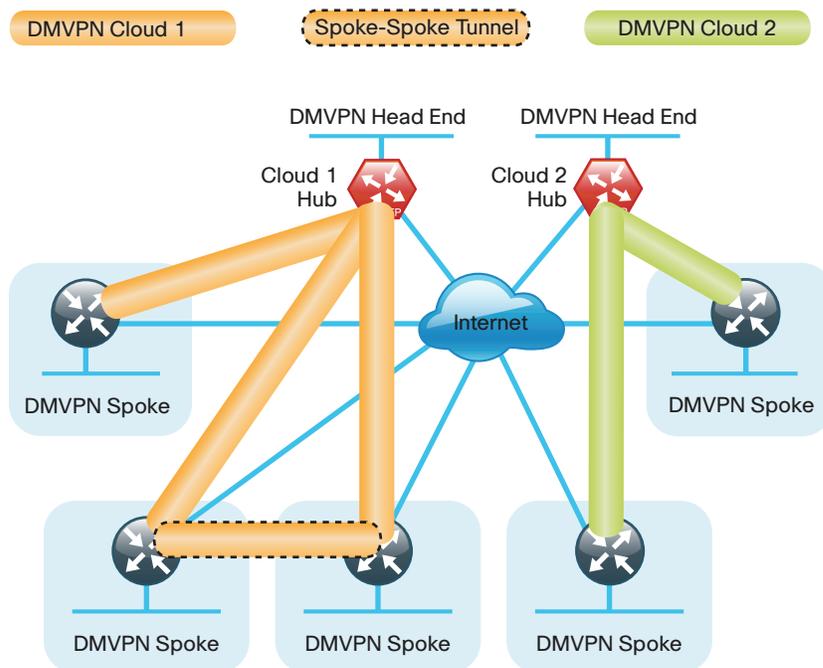
The single-link use cases in this design guide use Internet/DMVPN as a primary WAN transport that requires a DMVPN single-cloud, single-hub design. The dual-link use cases require a DMVPN dual-cloud design, each with a single hub router. The DMVPN routers use tunnel interfaces that support IP unicast as well as IP multicast and broadcast traffic, including the use of dynamic routing protocols. After the initial spoke-to-hub tunnel is active, it is possible to create dynamic spoke-to-spoke tunnels when site-to-site IP traffic flows require it.

The information required by a spoke to set up dynamic spoke-to-spoke tunnels and properly resolve other spokes is provided through the Next Hop Resolution Protocol (NHRP). Spoke-to-spoke tunnels allow for the optimal routing of traffic between locations without indirect forwarding through the hub. Idle spoke-to-spoke tunnels gracefully time out after a period of inactivity.

It is common for a firewall to be placed between the DMVPN hub routers and the Internet. In many cases, the firewall may provide Network Address Translation (NAT) from an internal RFC-1918 IP address (such as 10.4.128.33) to an Internet-routable IP address. The DMVPN solution works well with NAT but requires the use of IPsec transport mode to support a DMVPN hub behind static NAT.

DMVPN requires the use of Internet Security Association and Key Management Protocol (ISAKMP) keepalive intervals for Dead Peer Detection (DPD), which is essential to facilitate fast reconvergence and for spoke registration to function properly in case a DMVPN hub is reloaded. This design enables a spoke to detect that an encryption peer has failed and that the ISAKMP session with that peer is stale, which then allows a new one to be created. Without DPD, the IPsec security association (SA) must time out (the default is 60 minutes) and when the router cannot renegotiate a new SA, a new ISAKMP session is initiated. The maximum wait time is approximately 60 minutes.

Figure 20 - DMVPN dual-cloud



One of the key benefits of the DMVPN solution is that the spoke routers can use dynamically assigned addresses, often using DHCP from an Internet provider. The spoke routers can leverage an Internet default route for reachability to the hub routers and also other spoke addresses.

The DMVPN hub routers have static IP addresses assigned to their public-facing interfaces. This configuration is essential for proper operation as each of the spoke routers have these IP addresses embedded in their configurations.

# Deployment Details

The procedures in this section provide examples for some settings. The actual settings and values that you use are determined by your current network configuration. This process is used for the Dual DMVPN design (repeat for each DMVPN hub router), and also for the DMVPN Dedicated and DMVPN Dedicated Backup designs.

Table 11 - Parameters Used in the Deployment Examples

Hostname	Loopback IP Address	Port Channel IP Address
VPN-ASR1002-1	10.4.32.243/32	10.4.32.18/30
VPN-ASR1001-2	10.4.32.244/32	10.4.32.22/30

## PROCESS

### DMVPN Hub Router Configuration

1. Configure the Distribution Switch
2. Configure Connectivity to the LAN
3. Configure VRF Lite
4. Connect to Internet DMZ
5. Configure ISAKMP and IPsec
6. Configure the mGRE Tunnel
7. Configure EIGRP

#### Procedure 1 Configure the Distribution Switch



#### Reader Tip

This process assumes that the distribution switch has already been configured following the guidance in the [Campus Wired LAN Technology Design Guide](#). Only the procedures required to support the integration of the WAN aggregation router into the deployment are included.

The LAN distribution switch is the path to the organization's main campus and data center. A Layer 3 port-channel interface connects to the distribution switch to the WAN aggregation router and the internal routing protocol peers across this interface.



#### Tech Tip

As a best practice, use the same channel numbering on both sides of the link where possible.

**Step 1:** Configure the Layer 3 port-channel interface and assign the IP address.

```
interface Port-channel3
  description VPN-ASR1002-1
  no switchport
  ip address 10.4.32.17 255.255.255.252
  ip pim sparse-mode
  logging event link-status
  carrier-delay msec 0
  no shutdown
```

**Step 2:** Configure EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel using the **channel-group** command. The number for the port-channel and channel-group must match. Not all router platforms can support Link Aggregation Control Protocol (LACP) to negotiate with the switch, so EtherChannel is configured statically.

Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure traffic is prioritized appropriately.

```
interface GigabitEthernet1/0/3
  description VPN-ASR1002-1 Gig0/0/0
  !
interface GigabitEthernet2/0/3
  description VPN-ASR1002-1 Gig0/0/1
  !
interface range GigabitEthernet1/0/3, GigabitEthernet2/0/3
  no switchport
  macro apply EgressQoS
  carrier-delay msec 0
  channel-group 3 mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
```

**Step 3:** Allow the routing protocol to form neighbor relationships across the port channel interface.

```
router eigrp 100
  no passive-interface Port-channel3
```

**Step 4:** On the distribution layer switch, configure the Layer 3 interface connected to the LAN core to summarize the WAN network range.



### Tech Tip

It is a best practice to summarize IP routes from the WAN distribution layer towards the core.

```
interface Port-channel38
  description Link to C6500-VSS
  ip summary-address eigrp 100 10.4.32.0 255.255.248.0
  ip summary-address eigrp 100 10.4.128.0 255.255.240.0
  ip summary-address eigrp 100 10.4.160.0 255.255.252.0
  ip summary-address eigrp 100 10.5.0.0 255.255.0.0
```

**Step 5:** On the distribution layer switch, configure the layer 3 interfaces connected to the WAN aggregation routers to summarize the WAN remote-site network range.



### Tech Tip

It is a best practice to summarize IP routes from the WAN distribution layer towards the VPN WAN.

```
interface Port-channel3
  description VPN-ASR1002-1
  ip summary-address eigrp 100 10.5.0.0 255.255.0.0
```

Repeat this step as needed for additional WAN aggregation routers.

**Step 6:** Configure the WAN Aggregation Platform

Within this design, there are features and services that are common across all WAN aggregation routers. These are system settings that simplify and secure the management of the solution.

**Step 7:** Configure the device host name.

Configure the device host name to make it easy to identify the device.

```
hostname VPN-ASR1002-1
```

**Step 8:** Configure local login and password.

The local login account and password provides basic access authentication to a router which provides only limited operational privileges. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the disclosure of plain text passwords when viewing configuration files.

```
username admin password clsc0123
enable secret clsc0123
service password-encryption
aaa new-model
```

By default, https access to the router will use the enable password for authentication.

**Step 9:** (Optional) Configure centralized user authentication.

As networks scale in the number of devices to maintain it poses an operational burden to maintain local user accounts on every device. A centralized Authentication, Authorization and Accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined in Step 8 on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

**Step 10:** Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the network device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

Specify the transport preferred none on vty lines to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
  transport preferred none
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
  logging synchronous
```

Enable Simple Network Management Protocol (SNMP) to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

**Step 11:** (Optional) In networks where network operational support is centralized you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```



### Tech Tip

If you configure an access-list on the vty interface you may lose the ability to use ssh to login from one router to the next for hop-by-hop troubleshooting.

**Step 12:** Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organizations network.

You should program network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

**Step 13:** Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from the IP address block that the distribution switch summarizes to the rest of the network.

```
interface Loopback 0
  ip address 10.4.32.243 255.255.255.255
  ip pim sparse-mode
```

The **ip pim sparse-mode** command will be explained further in the process.

Bind the device processes for SNMP, SSH, PIM, TACACS+ and NTP to the loopback interface address for optimal resiliency:

```
snmp-server trap-source Loopback0
ip ssh source-interface Loopback0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

**Step 14:** Configure IP unicast routing.

EIGRP is configured facing the LAN distribution or core layer. In this design, the port-channel interface and the loopback must be EIGRP interfaces. The loopback may remain a passive interface. The network range must include both interface IP addresses, either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp 100
 network 10.4.0.0 0.1.255.255
 no auto-summary
 passive-interface default
 eigrp router-id 10.4.32.243
```

**Step 15:** Configure IP Multicast routing.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a Broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an IGMP message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as an RP to map the receivers to active sources so they can join their streams.

In this design, which is based on sparse mode multicast operation, Auto RP is used to provide a simple yet scalable way to provide a highly resilient RP environment.

Enable IP Multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

The Cisco ASR1000 Series router requires the **distributed** keyword.

```
ip multicast-routing distributed
```

Every Layer 3 switch and router must be configured to discover the IP Multicast RP with autorp. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

```
ip pim sparse-mode
```

## Procedure 2 Configure Connectivity to the LAN

Any links to adjacent distribution layers should be Layer 3 links or Layer 3 EtherChannels.

**Step 1:** Configure Layer 3 interface.

```
interface Port-channel3
  ip address 10.4.32.18 255.255.255.252
  ip pim sparse-mode
  no shutdown
```

**Step 2:** Configure EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel using the channel-group command. The number for the port-channel and channel-group must match.

```
interface GigabitEthernet0/0/0
  description WAN-D3750X Gig1/0/3
  !
interface GigabitEthernet0/0/1
  description WAN-D3750X Gig2/0/3
  !
interface range GigabitEthernet0/0/0, GigabitEthernet0/0/1
  no ip address
  channel-group 3
  cdp enable
  no shutdown
```

**Step 3:** Configure the EIGRP interface.

Allow EIGRP to form neighbor relationships across the interface to establish peering adjacencies and exchange route tables.

```
router eigrp 100
  no passive-interface Port-channel3
```

## Procedure 3 Configure VRF Lite

An Internet-facing VRF is created to support FVRF for DMVPN. The VRF name is arbitrary but it is useful to select a name that describes the VRF. An associated route descriptor (RD) must also be configured to make the VRF functional. The RD configuration also creates the routing and forwarding tables and associates the RD with the VRF instance.

This design uses VRF Lite so that the RD value can be chosen arbitrarily. It is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

```
ip vrf INET-PUBLIC
  rd 65512:1
```



## Tech Tip

Command Reference:

An RD is either ASN-related (composed of an ASN and an arbitrary number) or IP-address-related (composed of an IP address and an arbitrary number).

You can enter an RD in either of these formats:

*16-bit autonomous-system-number:your 32-bit number*

For example, 65512:1.

*32-bit IP address: your 16-bit number*

For example, 192.168.122.15:1.

## Procedure 4 Connect to Internet DMZ

The DMVPN hub requires a connection to the Internet, and in this design the DMVPN hub is connected through a Cisco ASA5500 Adaptive Security Appliance using a DMZ interface specifically created and configured for a VPN termination router.

**Step 1:** Enable the interface, select the VRF, and assign the IP address.

The IP address that you use for the Internet-facing interface of the DMVPN hub router must be an Internet routable address. There are two possible methods to accomplish this task:

- Assign a routable IP address directly to the router
- Assign a non-routable RFC-1918 address directly to the router and use a static NAT on the Cisco ASA5500 to translate the router IP address to a routable IP address.

This design assumes that the Cisco ASA5500 is configured for static NAT for the DMVPN hub router.

The DMVPN design is using FVRF, so this interface must be placed into the VRF configured in the previous procedure.

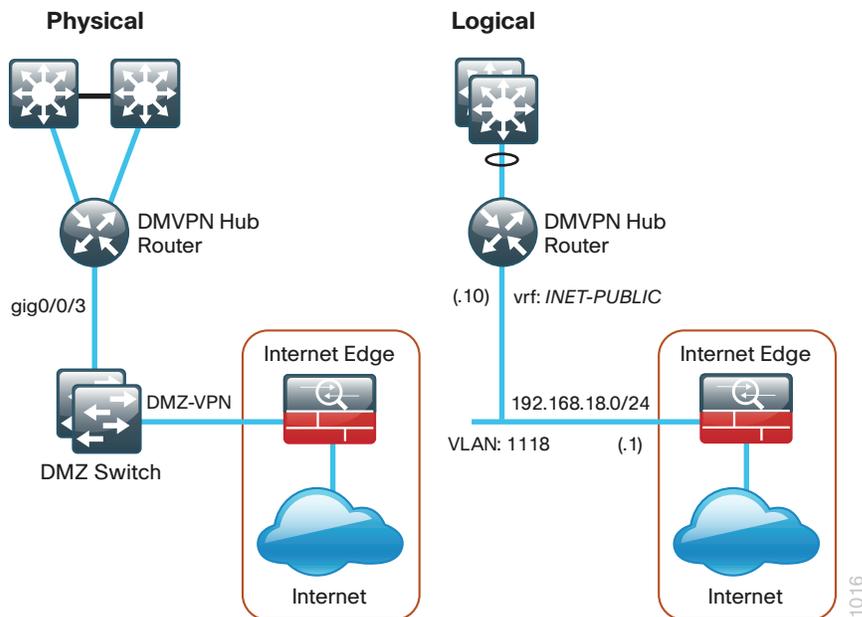
```
interface GigabitEthernet0/0/3
  ip vrf forwarding INET-PUBLIC
  ip address 192.168.18.10 255.255.255.0
  no shutdown
```

**Step 2:** Configure the VRF specific default routing.

The VRF created for FVRF must have its own default route to the Internet. This default route points to the ASA5500 DMZ interface IP address.

```
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 192.168.18.1
```

Figure 21 - Physical and logical views for DMZ connection



## Procedure 5 Configure ISAKMP and IPsec

**Step 1:** Configure the crypto keyring.

The crypto keyring defines a pre-shared key (or password) valid for IP sources that are reachable within a particular VRF. This key is a wildcard pre-shared key if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

**Step 2:** Configure the ISAKMP policy.

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Standard (SHA)
- Authentication by Pre-Shared Key (PSK)
- Diffie-Hellman group: 2

```
crypto isakmp policy 10
encr aes 256
hash sha
authentication pre-share
group 2
```

**Step 3:** Create the ISAKMP Profile.

The ISAKMP profile creates an association between an identity address, a VRF, and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
  keyring DMVPN-KEYRING
  match identity address 0.0.0.0 INET-PUBLIC
```

**Step 4:** Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
mode transport
```

**Step 5:** Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
```

## Procedure 6 Configure the mGRE Tunnel

Table 12 - DMVPN Tunnel Parameters

DMVPN cloud	Tunnel IP address	EIGRP AS	NHRP network ID
Primary	10.4.34.1/23	200	101
Secondary	10.4.36.1/23	201	102

**Step 1:** Configure basic interface settings.

Tunnel interfaces are created as they are configured. The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

The bandwidth setting should be set to match the Internet bandwidth of the respective primary or secondary carrier.

Configure the IP MTU to 1400 and the ip tcp adjust-mss to 1360. There is a 40 byte difference which corresponds to the combined IP and TCP header length.

```
interface Tunnel10
  bandwidth 10000
  ip address 10.4.34.1 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip tcp adjust-mss 1360
```

**Step 2:** Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. Use the same source interface that you use to connect to the Internet. Set the **tunnel vrf** command to the VRF defined previously for FVRF.

Enabling encryption on this interface requires the application of the IPsec profile configured in the previous procedure.

```
interface Tunnel10
  tunnel source GigabitEthernet0/0/3
  tunnel mode gre multipoint
  tunnel vrf INET-PUBLIC
  tunnel protection ipsec profile DMVPN-PROFILE
```

**Step 3:** Configure NHRP.

The DMVPN hub router acts in the role of NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. The NHRP cache holdtime should be configured to 600 seconds.

EIGRP (configured in the following procedure) relies on a multicast transport and requires NHRP to automatically add routers to the multicast NHRP mappings.

The **ip nhrp redirect** command allows the DMVPN hub to notify spoke routers that a more optimal path may exist to a destination network, which may be required for DMVPN spoke-spoke direct communications.

```
interface Tunnel10
  ip nhrp authentication cisco123
  ip nhrp map multicast dynamic
  ip nhrp network-id 101
  ip nhrp holdtime 600
  ip nhrp redirect
```

**Step 4:** Enable PIM non-broadcast multiple access (NBMA) mode for the DMVPN tunnel.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This inability to directly exchange information can also cause problems when running IP Multicast.

To resolve this issue requires a method where each remote PIM neighbor has its join messages tracked separately. A router in PIM NBMA mode treats each remote PIM neighbor as if it were connected to the router through a point-to-point link.



### Tech Tip

Do not enable PIM on the Internet DMZ interface, as no multicast traffic should be requested from this interface.

```
interface Tunnel10
  ip pim sparse-mode
  ip pim nbma-mode
```

#### Step 5: Configure EIGRP.

You configure EIGRP in the following Procedure 8, but there are some specific requirements for the mGRE tunnel interface that you need to configure first.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This limitation requires that the DMVPN hub router advertise routes from other spokes on the same network. This advertisement of these routes would normally be prevented by split horizon, and can be overridden by the **no ip split-horizon eigrp** command.

The EIGRP hello interval is increased to 20 seconds and the EIGRP hold time is increased to 60 seconds to accommodate up to 500 remote sites on a single DMVPN cloud.

```
interface Tunnel10
  ip hello-interval eigrp [EIGRP AS] 20
  ip hold-time eigrp [EIGRP AS] 60
  no ip split-horizon eigrp [EIGRP AS]
```

### Procedure 7 Configure EIGRP

You use two EIGRP processes on the DMVPN hub routers. The primary reason for the additional process is to ensure that routes learned from the WAN remotes appear as EIGRP external routes on the WAN distribution switch. If you used only a single process, the remote-site routes would appear as EIGRP internal routes on the WAN distribution switch, which would be preferred to any MPLS VPN learned routes.

#### Step 1: Enable an additional EIGRP process for DMVPN.

Configure EIGRP for the DMVPN mGRE interface. Routes from the other EIGRP process are redistributed. Because the routing protocol is the same, no default metric is required.

The tunnel interface is the only EIGRP interface, and you need to explicitly list its network range.

```
router eigrp [EIGRP AS]
  network 10.4.34.0 0.0.1.255
  passive-interface default
  no passive-interface Tunnel10
  eigrp router-id 10.4.32.243
  no auto-summary
```

**Step 2:** Tag and redistribute the routes.

This design uses mutual route redistribution. DMVPN Routes from the EIGRP-200/EIGRP201 process are redistributed into EIGRP-100 and other learned routes from EIGRP-100 are redistributed into EIGRP-200/EIGRP-201. Because the routing protocol is the same, no default metric is required.

It is important to tightly control how routing information is shared between different routing protocols when this mutual route redistribution is used; otherwise, it is possible to experience route flapping, where certain routes are repeatedly installed and with-drawn from the device routing tables. Proper route control ensures the stability of the routing table.

An inbound distribute-list is used on the WAN-aggregation routers to limit which routes are accepted for installation into the route table. These routers are configured to only accept routes which do not originate from the MPLS and DMVPN WAN sources. To accomplish this task, the DMVPN learned WAN routes must be explicitly tagged by their DMVPN hub router during the route redistribution process. The specific route tags in use are shown in the following table.

*Table 13 - Route tag information for DMVPN hub router*

Tag	Route source	Tag method	Action
65401	MPLS A	implicit	accept
65402	MPLS B	implicit	accept
300	Layer 2 WAN	explicit	accept
65512	DMVPN hub routers	explicit	tag

This example includes all WAN route sources in the reference design. Depending on the actual design of your network, you might need to use more tags.

```
router eigrp 100
 redistribute eigrp [EIGRP AS] route-map SET-ROUTE-TAG-DMVPN
!
router eigrp [EIGRP AS]
 redistribute eigrp 100
!
route-map SET-ROUTE-TAG-DMVPN permit 10
 match interface Tunnel10
 set tag 65512
```

## Firewall and DMZ Switch Configuration

1. Configure the DMZ Switch
2. Configure Firewall DMZ Interface
3. Configure Network Address Translation
4. Configure Security Policy

### Procedure 1 Configure the DMZ Switch



#### Reader Tip

This procedure assumes that the switch has already been configured following the guidance in the [Campus Wired LAN Technology Design Guide](#). Only the procedures required to support the integration of the firewall into the deployment are included.

**Step 1:** Set the DMZ switch to be the spanning tree root for the VLAN that contains the DMVPN hub router.

```
vlan 1118
spanning-tree vlan 1118 root primary
```

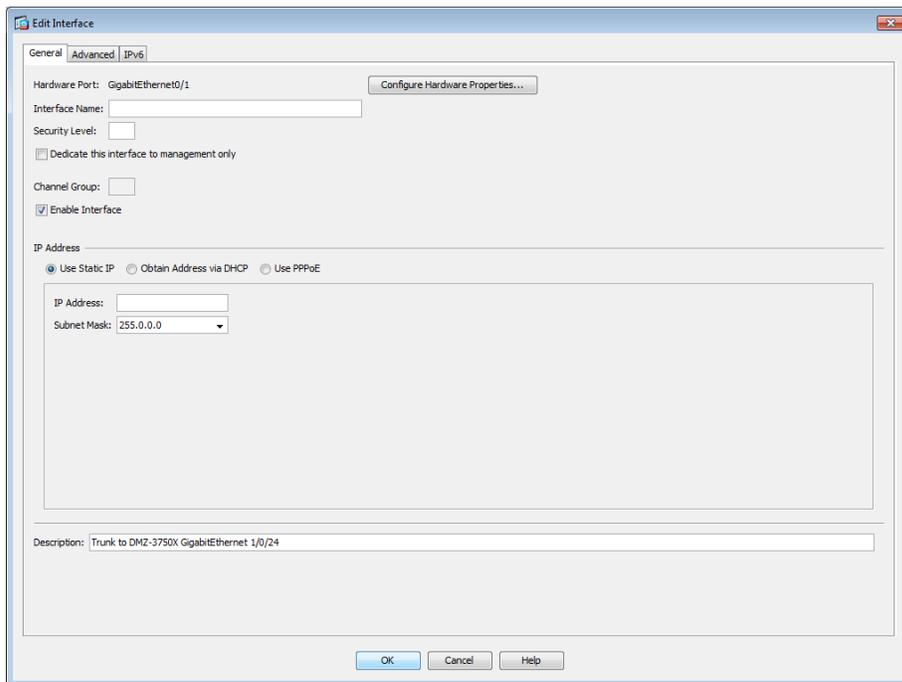
**Step 2:** Configure the interfaces that are connected to the appliances as a trunk.

```
interface GigabitEthernet1/0/24
description IE-ASA5540a Gig0/1
!
interface GigabitEthernet2/0/24
description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 1118
switchport mode trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```



**Step 2:** Click **Edit**.

**Step 3:** Select **Enable Interface**, and then click **OK**.



**Step 4:** On the Interface pane, click **Add > Interface**.

**Step 5:** In the **Hardware Port** list choose the interface configured in Step 1.(Example: GigabitEthernet0/1)

**Step 6:** In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1118)

**Step 7:** In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1118)

**Step 8:** Enter an **Interface Name**. (Example: dmz-dmvpn)

**Step 9:** In the **Security Level** box, enter a value of **75**.

**Step 10:** Enter the interface **IP Address**. (Example: 192.168.18.1)

**Step 11:** Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

Step 12: Click Apply.

The screenshot shows the 'Add Interface' configuration window. The 'General' tab is selected. The configuration includes:

- Hardware Port: GigabitEthernet0/1
- VLAN ID: 1118
- Subinterface ID: 1118
- Interface Name: dmz-dmvpn
- Security Level: 75
- Dedicate this interface to management only
- Channel Group:
- Enable Interface
- IP Address section:
  - Use Static IP
  - Obtain Address via DHCP
  - Use PPPoE
  - IP Address: 192.168.18.1
  - Subnet Mask: 255.255.255.0
- Description: DMVPN aggregation router connections on VLAN 1118

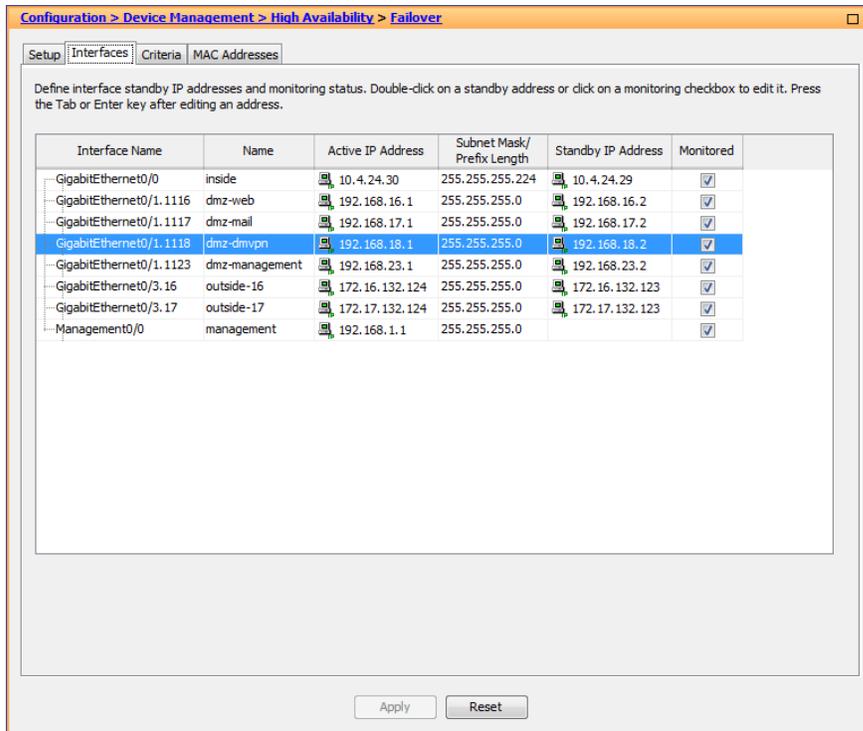
Buttons: OK, Cancel, Help

Step 13: In Configuration > Device Management > High Availability > click Failover.

Step 14: On the **Interfaces** tab, for the interface created in Step 4, enter the IP address of the standby unit in the **Standby IP address** column. (Example: 192.168.18.2)

Step 15: Select **Monitored**.

Step 16: Click Apply.



### Procedure 3 Configure Network Address Translation

The DMZ network uses private network (RFC 1918) addressing that is not Internet routable, so the firewall must translate the DMZ address of the DMVPN hub router to an outside public address.

The example DMZ address to public IP address mapping is shown in the following table.

DMVPN hub router DMZ address	DMVPN hub router public address (externally routable after NAT)
192.168.18.10	172.16.130.1 (ISP-A)
192.168.18.11	172.17.130.1 (ISP-B)

**Step 1:** In Configuration > Firewall > Objects > click Network Objects/Groups.

First, add a network object for the public address of the DMVPN hub router on the primary internet connection.

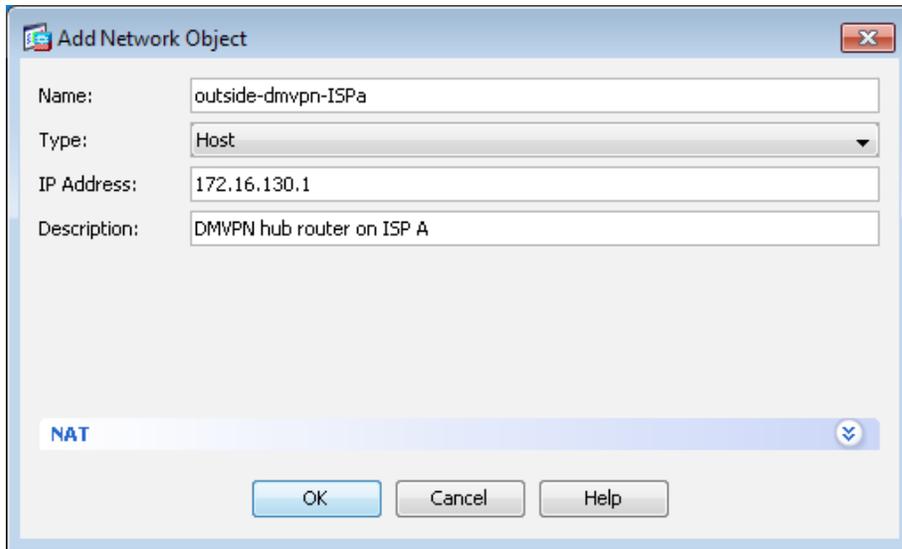
**Step 2:** Click Add > Network Object.

**Step 3:** On the Add Network Object dialog box, in the **Name box**, enter a description for the DMVPN hub router's public IP address. (Example: outside-dmvpn-ISPa)

**Step 4:** In the **Type** list, choose **Host**.

**Step 5:** In the **IP Address** box, enter the DMVPN hub router's public IP address, and then click **OK**. (Example: 172.16.130.1)

**Step 6:** Click **Apply**.



The screenshot shows a dialog box titled "Add Network Object". It has a close button in the top right corner. The dialog contains the following fields and values:

- Name:** outside-dmvpn-ISPa
- Type:** Host (selected in a dropdown menu)
- IP Address:** 172.16.130.1
- Description:** DMVPN hub router on ISP A

At the bottom of the dialog, there is a section labeled "NAT" with a dropdown arrow. Below this section are three buttons: "OK", "Cancel", and "Help".

Next, you add a network object for the private DMZ address of the DMVPN hub router.

**Step 7:** Click **Add > Network Object**.

**Step 8:** On the **Add Network Object** dialog box, in the **Name box**, enter a description for the DMVPN hub router's private DMZ IP address. (Example: dmz-dmvpn-1)

**Step 9:** In the **Type** list, choose **Host**.

**Step 10:** In the **IP Address** box, enter the router's private DMZ IP address. (Example: 192.168.18.10)

**Step 11:** Click the two down arrows. The NAT pane expands.

**Step 12:** Select **Add Automatic Address Translation Rules**.

**Step 13:** In the **Translated Addr** list, choose the network object created in Step 2 (Example: outside-dmvpn-ISPa).

**Step 14:** Select **Use one-to-one address translation**, and then click **OK**.

The screenshot shows the 'Add Network Object' dialog box. The fields are filled with the following information:

- Name: dmz-dmvpn-1
- Type: Host
- IP Version: IPv4 (selected)
- IP Address: 192.168.18.10
- Description: NAT the primary DMVPN hub router in the DMZ to ISP A

The 'NAT' section is expanded and shows the following options:

- Add Automatic Address Translation Rules
- Type: Static
- Translated Addr: outside-dmvpn-ISPa
- Use one-to-one address translation
- PAT Pool Translated Address: [empty]
- Round Robin
- Extend PAT uniqueness to per destination instead of per interface
- Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023
- Fall through to interface PAT(dest intf): IPS-mgmt
- Use IPv6 for interface PAT

Buttons at the bottom include 'Advanced...', 'OK', 'Cancel', and 'Help'.

**Step 15:** Repeat this process for the resilient DMVPN hub router.

## Procedure 4 Configure Security Policy

The DMVPN DMZ provides an additional layer of protection to lower the likelihood of certain types of misconfiguration of the DMVPN routers exposing the business network to the Internet. A filter allows only DMVPN related traffic to reach the DMVPN hub routers.

Table 14 - Required DMVPN protocols (aggregation router)

Name	Protocol	Usage
non500-isakmp	UDP 4500	IPsec via NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec

Table 15 - Optional protocols—DMVPN hub router

Name	Protocol	Usage
icmp echo	ICMP Type 0, Code 0	Allow remote pings
icmp echo-reply	ICMP Type 8, Code 0	Allow ping replies (from our requests)
icmp ttl-exceeded	ICMP Type 11, Code 0	Allow traceroute replies (from our requests)
icmp port-unreachable	ICMP Type 3, Code 3	Allow traceroute replies (from our requests)
UDP high ports	UDP > 1023	Allow remote traceroute

**Step 1:** Navigate to **Configuration > Firewall > Access Rules**.

**Step 2:** Expand the Global rules, and within the Global rules click the rule that denies traffic from the DMZ toward other networks.



Next, you must insert a new rule above the rule you selected.

**Step 3:** Click **Add > Insert**.

You must enable the DMVPN remote routers to communicate with the DMVPN hub routers in the DMZ.

**Step 4:** In the **Destination** list, choose the network object group created in Procedure 3. (Example: dmz-dmvpn-network/24)

**Step 5:** In the **Service** list box, enter **esp, udp/4500, udp/isakmp**, and then click **OK**.

**Add Access Rule**

Interface: -- Any --

Action:  Permit  Deny

Source Criteria

Source: any4

User:

Security Group:

Destination Criteria

Destination: dmz-dmvpn-network/24

Security Group:

Service: esp, udp/4500, udp/isakmp

Description: Allow traffic to the DMVPN hub routers

Enable Logging

Logging Level: Default

**More Options**

OK Cancel Help

Next, you must insert a new rule to allow diagnostic traffic to the DMVPN hub routers.

**Step 6:** Click **Add > Insert**.

You must enable the DMVPN remote routers to send diagnostics to the DMVPN hub routers in the DMZ.

**Step 7:** In the **Destination** list, choose the automatically created network object for the DMVPN DMZ. (Example: dmz-dmvpn-network/24)

**Step 8:** In the **Service** list box, enter **icmp/echo, icmp/echo-reply**, and then click **OK**.

Interface: -- Any --  
Action:  Permit  Deny

Source Criteria

Source: any4  
User:  
Security Group:

Destination Criteria

Destination: dmz-dmvpn-network/24  
Security Group:  
Service: icmp/echo, icmp/echo-reply

Description: Allow diagnostic traffic to the DMVPN hub routers

Enable Logging  
Logging Level: Default

More Options

OK Cancel Help

**Step 9:** Click **Apply**.

## PROCESS

### Adding DMVPN Hub to Existing WAN-Aggregation Router

1. Configure ISAKMP and IPsec
2. Configure the mGRE Tunnel
3. Configure EIGRP
4. Configure NAT on the Firewall
5. Configure Security Policy on the Firewall

A smaller scale deployment of VPN backup may use the existing MPLS WAN router as the DMVPN hub router. This process assumes that the MPLS WAN router is already configured, and is using static routing with the MPLS carrier. This process is used for the DMVPN Shared Backup designs.



#### Tech Tip

This process does not require FVRF.

## Procedure 1 Configure ISAKMP and IPsec

**Step 1:** Configure the crypto keyring.

The crypto keyring defines a pre-shared key (or password) valid for IP sources. This key is a wildcard pre-shared key if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

**Step 2:** Configure the ISAKMP policy.

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Standard (SHA)
- Authentication by Pre-Shared Key (PSK)
- Diffie-Hellman group: 2

```
crypto isakmp policy 10
  encr aes 256
  hash sha
  authentication pre-share
  group 2
```

**Step 3:** Create the ISAKMP Profile.

The ISAKMP profile creates an association between an identity address, a VRF, and a crypto keyring. A wildcard address is referenced with 0.0.0.0.

```
crypto isakmp profile ISAKMP-PROFILE
  keyring DMVPN-KEYRING
  match identity address 0.0.0.0
```

**Step 4:** Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
  mode transport
```

**Step 5:** Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile ISAKMP-PROFILE
```

## Procedure 2 Configure the mGRE Tunnel

Table 16 - DMVPN Tunnel Parameters

DMVPN cloud	Tunnel IP address	EIGRP AS	NHRP network ID
Primary	10.4.34.1/24	200	101

**Step 1:** Configure basic interface settings.

Tunnel interfaces are created as they are configured. The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

The bandwidth setting should be set to match the Internet bandwidth of the respective primary or secondary carrier.

Configure the IP MTU to 1400 and the ip tcp adjust-mss to 1360. There is a 40 byte difference which corresponds to the combined IP and TCP header length.

```
interface Tunnel10
  bandwidth 10000
  ip address 10.4.34.1 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip tcp adjust-mss 1360
```

**Step 2:** Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. Use the same source interface that you use to connect to the Internet.

Enabling encryption on this interface requires the application of the IPsec profile configured in the previous procedure.

```
interface Tunnel10
  tunnel source Port-Channel132
  tunnel mode gre multipoint
  tunnel protection ipsec profile DMVPN-PROFILE
```

**Step 3:** Configure NHRP.

The DMVPN hub router acts in the role of NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. The NHRP cache holdtime should be configured to 600 seconds.

EIGRP (configured in the following procedure) relies on a multicast transport and requires NHRP to automatically add routers to the multicast NHRP mappings.

The **ip nhrp redirect** command allows the DMVPN hub to notify spoke routers that a more optimal path may exist to a destination network, which may be required for DMVPN spoke-to-spoke direct communications.

```
interface Tunnel10
  ip nhrp authentication cisco123
  ip nhrp map multicast dynamic
  ip nhrp network-id 101
  ip nhrp holdtime 600
  ip nhrp redirect
```

**Step 4:** Enable PIM non-broadcast multiple access (NBMA) mode for the DMVPN tunnel.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This inability to directly exchange information can also cause problems when running IP Multicast.

To resolve this issue requires a method where each remote PIM neighbor has its join messages tracked separately. A router in PIM NBMA mode treats each remote PIM neighbor as if it were connected to the router through a point-to-point link.



#### Tech Tip

Do not enable PIM on the Internet DMZ interface, as no multicast traffic should be requested from this interface.

```
interface Tunnel10
  ip pim sparse-mode
  ip pim nbma-mode
```

**Step 5:** Configure EIGRP.

You configure EIGRP in the following Procedure 3, but there are some specific requirements for the mGRE tunnel interface that you need to configure first.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This limitation requires that the DMVPN hub router advertise routes from other spokes on the same network. This advertisement of these routes would normally be prevented by split horizon, and can be overridden by the **no ip split-horizon eigrp** command.

The EIGRP hello interval is increased to 20 seconds and the EIGRP hold time is increased to 60 seconds to accommodate up to 500 remote sites on a single DMVPN cloud.

```
interface Tunnel10
  ip hello-interval eigrp 200 20
  ip hold-time eigrp 200 60
  no ip split-horizon eigrp 200
```

### Procedure 3 Configure EIGRP

You use two EIGRP processes on the DMVPN hub routers. The primary reason for the additional process is to ensure that routes learned from the WAN remotes appear as EIGRP external routes on the WAN distribution switch. If you used only a single process, the remote-site routes would appear as EIGRP internal routes on the WAN distribution switch, which would be preferred to any MPLS VPN learned routes.

**Step 1:** Enable an additional EIGRP process for DMVPN.

Configure EIGRP-200 for the DMVPN mGRE interface. Routes from the other EIGRP process are redistributed. Because the routing protocol is the same, no default metric is required.

The tunnel interface is the only EIGRP interface, and you need to explicitly list its network range.

```
router eigrp 200
 network 10.4.34.0 0.0.0.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.4.32.254
 no auto-summary
```

**Step 2:** Tag and redistribute the routes.

This design uses mutual route redistribution. DMVPN Routes from the EIGRP-200 process are redistributed into EIGRP-100 and other learned routes from EIGRP-100 are redistributed into EIGRP-200. Because the routing protocol is the same, no default metric is required.

It is important to tightly control how routing information is shared between different routing protocols when this mutual route redistribution is used; otherwise, it is possible to experience route flapping, where certain routes are repeatedly installed and with-drawn from the device routing tables. Proper route control ensures the stability of the routing table.

An inbound distribute-list may be used on the WAN-aggregation routers to limit which routes are accepted for installation into the route table. These routers are configured to only accept routes which do not originate from the MPLS and DMVPN WAN sources. To accomplish this task, the DMVPN learned WAN routes must be explicitly tagged by their DMVPN hub router during the route redistribution process.

This example includes all WAN route sources in the reference design. Depending on the actual design of your network, you might need to use more tags.

```
router eigrp 100
 redistribute eigrp 200 route-map SET-ROUTE-TAG-DMVPN
!
router eigrp 200
 redistribute eigrp 100
!
route-map SET-ROUTE-TAG-DMVPN permit 10
 match interface Tunnel10
 set tag 65512
```

## Procedure 4 Configure NAT on the Firewall



### Reader Tip

This procedure assumes that the firewall has already been configured following the guidance in the [Firewall and IPS Technology Design Guide](#). Only the procedures required to allow VPN protocols through the firewall are included.

The DMVPN hub router is connected to the network core, behind the Internet edge firewall. The Internet Edge ASA must forward all incoming VPN traffic to the router's private IP address and accommodate the VPN traffic in the ASA's outside-to-inside access policy.

The internal network uses private network (RFC 1918) addressing that is not Internet routable, so the firewall must translate the core/distribution facing address of the DMVPN hub router to an outside public address.

The example internal address to public IP address mapping is shown in the following table.

DMVPN hub router internal address	DMVPN hub router public address (externally routable after NAT)
10.4.32.2	172.16.130.1

**Step 1:** In **Configuration > Firewall > Objects >** click **Network Objects/Groups**.

First, add a network object for the public address of the DMVPN hub router on the internet connection.

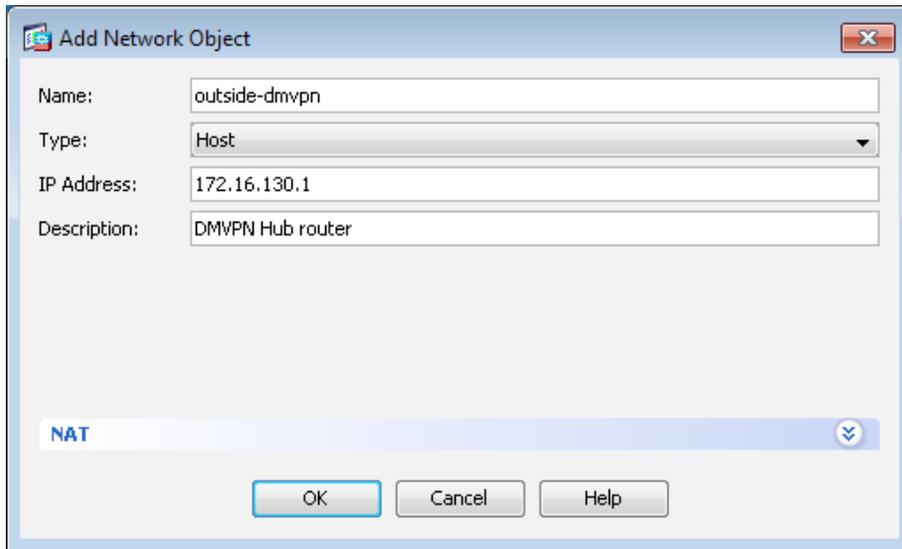
**Step 2:** Click **Add > Network Object**.

**Step 3:** On the Add Network Object dialog box, in the **Name box**, enter a description for the DMVPN hub router's public IP address. (Example: outside-dmvpn)

**Step 4:** In the **Type** list, choose **Host**.

**Step 5:** In the **IP Address** box, enter the DMVPN hub router's public IP address, and then click **OK**. (Example: 172.16.130.1)

**Step 6:** Click **Apply**.



The screenshot shows a dialog box titled "Add Network Object". It has a close button in the top right corner. The dialog contains the following fields and controls:

- Name:** A text box containing "outside-dmvpn".
- Type:** A dropdown menu with "Host" selected.
- IP Address:** A text box containing "172.16.130.1".
- Description:** A text box containing "DMVPN Hub router".
- NAT:** A section with a blue header and a dropdown arrow pointing down.
- Buttons:** "OK", "Cancel", and "Help" buttons at the bottom.

Next, you add a network object for the private internal address of the DMVPN hub router.

**Step 7:** Click **Add > Network Object**.

**Step 8:** On the **Add Network Object** dialog box, in the **Name box**, enter a description for the DMVPN hub router's private internal IP address. (Example: internal-dmvpn-1)

**Step 9:** In the **Type** list, choose **Host**.

**Step 10:** In the **IP Address** box, enter the router's private internal IP address. (Example: 10.4.32.2)

**Step 11:** Click the two down arrows. The NAT pane expands.

**Step 12:** Select **Add Automatic Address Translation Rules**.

**Step 13:** In the **Translated Addr** list, choose the network object created in Step 2.

Step 14: Select **Use one-to-one address translation**, and then click **OK**.

The screenshot shows the 'Add Network Object' dialog box. The fields are filled as follows:

- Name: inside-dmvpn
- Type: Host
- IP Version: IPv4 (selected)
- IP Address: 10.4.32.2
- Description: NAT the DMVPN hub router internal address to the outside address

The NAT section is expanded and shows the following options:

- Add Automatic Address Translation Rules
- Type: Static
- Translated Addr: outside-dmvpn
- Use one-to-one address translation
- PAT Pool Translated Address: [empty]
- Round Robin
- Extend PAT uniqueness to per destination instead of per interface
- Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023
- Fall through to interface PAT(dest intf): IPS-mgmt
- Use IPv6 for interface PAT

Buttons at the bottom include 'Advanced...', 'OK', 'Cancel', and 'Help'.

Step 15: Click **Apply**.

## Procedure 5 Configure Security Policy on the Firewall

A filter allows only DMVPN related traffic to reach the DMVPN hub router.

Table 17 - Required DMVPN protocols (aggregation router)

Name	Protocol	Usage
non500-isakmp	UDP 4500	IPsec via NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec

Table 18 - Optional protocols—DMVPN hub router

Name	Protocol	Usage
icmp echo	ICMP Type 0, Code 0	Allow remote pings
icmp echo-reply	ICMP Type 8, Code 0	Allow ping replies (from our requests)
icmp ttl-exceeded	ICMP Type 11, Code 0	Allow traceroute replies (from our requests)
icmp port-unreachable	ICMP Type 3, Code 3	Allow traceroute replies (from our requests)
UDP high ports	UDP > 1023	Allow remote traceroute

**Step 1:** Navigate to **Configuration > Firewall > Access Rules**.

**Step 2:** Expand the Global rules, and within the Global rules click the final rule that implicitly denies traffic from any to any.



Next, you must add a new rule above the rule you selected.

**Step 3:** Click **Add > Add Access Rule**.

You must enable the DMVPN remote routers to communicate with the DMVPN hub router on the internal network.

**Step 4:** In the **Destination** list, choose the host network object created in Procedure 4. (Example: inside-dmvpn)

**Step 5:** In the **Service** list box, enter **esp, udp/4500, udp/isakmp**, and then click **OK**.

The screenshot shows the 'Add Access Rule' dialog box. The 'Interface' is set to '-- Any --'. The 'Action' is set to 'Permit'. Under 'Source Criteria', 'Source' is 'any4', 'User' is empty, and 'Security Group' is empty. Under 'Destination Criteria', 'Destination' is 'inside-dmvpn', 'Security Group' is empty, and 'Service' is 'esp, udp/4500, udp/isakmp'. The 'Description' field contains 'Allow traffic to the DMVPN hub router'. The 'Enable Logging' checkbox is checked, and the 'Logging Level' is set to 'Default'. There is a 'More Options' section with a dropdown arrow. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Next, you must add a new rule to allow diagnostic traffic to the DMVPN hub routers.

**Step 6:** Click **Add > Add Access Rule**.

You must enable the DMVPN remote routers to send diagnostic traffic to the DMVPN hub router.

**Step 7:** In the **Destination** list, choose the host network object created in Procedure 4. (Example: inside-dmvpn)

**Step 8:** In the **Service** list box, enter **icmp/echo, icmp/echo-reply**, and then click **OK**.

**Add Access Rule**

Interface: -- Any --

Action:  Permit  Deny

Source Criteria

Source: any4

User:

Security Group:

Destination Criteria

Destination: inside-dmvpn

Security Group:

Service: icmp/echo, icmp/echo-reply

Description: Allow diagnostic traffic to the DMVPN hub router

Enable Logging

Logging Level: Default

**More Options**

OK Cancel Help

**Step 9:** Click **Apply**.

## Remote-Site DMVPN Spoke Router Configuration

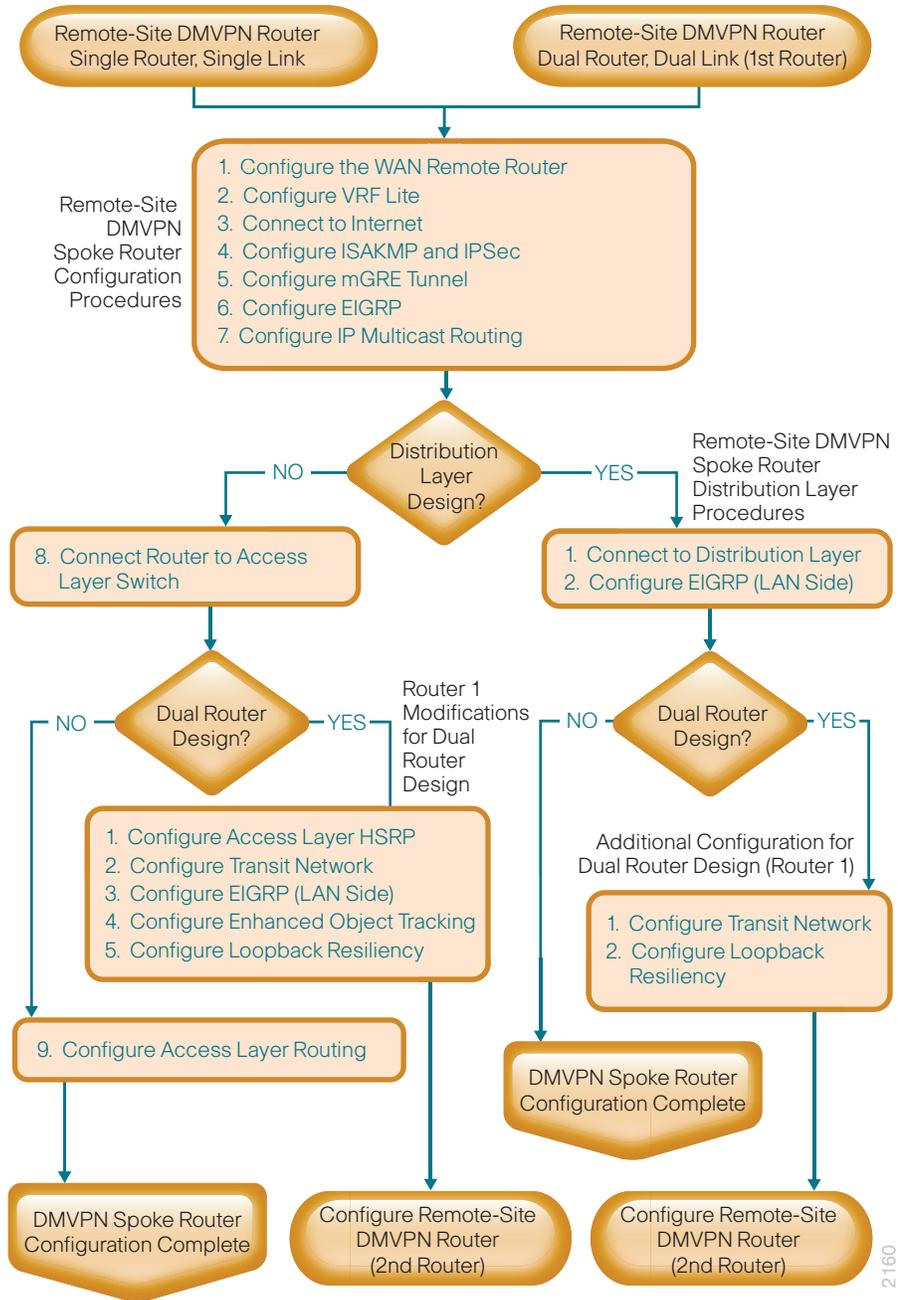
1. Configure the WAN Remote Router
2. Configure VRF Lite
3. Connect to the Internet
4. Configure ISAKMP and IPsec
5. Configure the mGRE Tunnel
6. Configure EIGRP
7. Configure IP Multicast Routing
8. Connect Router to Access Layer Switch
9. Configure Access Layer Routing

This set of procedures is for the configuration of a DMVPN spoke router for a DMVPN remote site (single-router, single-link) and includes all required procedures.

You should also use this set of procedures when you configure a DMVPN + DMVPN remote site. Use these procedures when you configure the first router of the dual-router, dual-link design.

The following flowchart provides details about how to complete the configuration of a remote-site DMVPN spoke router.

Figure 23 - Remote-site DMVPN spoke router configuration flowchart



## Procedure 1 Configure the WAN Remote Router

Within this design, there are features and services that are common across all WAN remote site routers. These are system settings that simplify and secure the management of the solution.

**Step 1:** Configure the device host name to make it easy to identify the device.

```
hostname [hostname]
```

**Step 2:** Configure local login and password.

The local login account and password provides basic access authentication to a router which provides only limited operational privileges. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the disclosure of plain text passwords when viewing configuration files.

```
username admin password cisco123
enable secret cisco123
service password-encryption
aaa new-model
```

By default, https access to the router will use the enable password for authentication.

**Step 3:** (Optional) Configure centralized user authentication.

As networks scale in the number of devices to maintain it poses an operational burden to maintain local user accounts on every device. A centralized Authentication, Authorization and Accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

**Step 4:** Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the network device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

Specify the transport preferred none on vty lines to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
  transport preferred none
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
  logging synchronous
```

Enable Simple Network Management Protocol (SNMP) to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

**Step 5:** (Optional) In networks where network operational support is centralized you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```



### Tech Tip

If you configure an access-list on the vty interface you may lose the ability to use ssh to login from one router to the next for hop-by-hop troubleshooting.

**Step 6:** Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organizations network.

You should program network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

**Step 7:** Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from a unique network range that is not part of any other internal network summary range.

```
interface Loopback 0
 ip address [ip address] 255.255.255.255
 ip pim sparse-mode
```

The **ip pim sparse-mode** command will be explained in the next step.

Bind the device processes for SNMP, SSH, PIM, TACACS+ and NTP to the loopback interface address for optimal resiliency:

```
snmp-server trap-source Loopback0
ip ssh source-interface Loopback0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

**Step 8:** Configure IP Multicast routing.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a Broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an IGMP message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as an RP to map the receivers to active sources so they can join their streams.

In this design, which is based on sparse mode multicast operation, Auto RP is used to provide a simple yet scalable way to provide a highly resilient RP environment.

Enable IP Multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

Every Layer 3 switch and router must be configured to discover the IP Multicast RP with autorp. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

```
ip pim sparse-mode
```

## Procedure 2 Configure VRF Lite

An Internet-facing VRF is created to support FVRF for DMVPN. The VRF name is arbitrary but it is useful to select a name that describes the VRF. An associated RD must also be configured to make the VRF functional. The RD configuration also creates the routing and forwarding tables and associates the RD with the VRF instance.

This design uses VRF Lite so that the RD value can be chosen arbitrarily. It is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

```
ip vrf INET-PUBLIC1  
rd 65512:1
```



### Tech Tip

Command Reference:

An RD is either ASN-related (composed of an ASN and an arbitrary number) or IP-address-related (composed of an IP address and an arbitrary number).

You can enter an RD in either of these formats:

*16-bit autonomous-system-number:your 32-bit number*

For example, 65512:1.

*32-bit IP address: your 16-bit number*

For example, 192.168.122.15:1.

## Procedure 3 Connect to the Internet

The remote sites that are using DMVPN can use either static or dynamically assigned IP addresses. Cisco tested the design with a DHCP assigned external address, which also provides a dynamically configured default route.

The DMVPN spoke router connects directly to the Internet without a separate firewall. This connection is secured in two ways. Because the Internet interface is in a separate VRF, no traffic can access the global VRF except traffic sourced through the DMVPN tunnel. This design provides implicit security. Additionally, an IP access list permits only the traffic required for an encrypted tunnel, as well as DHCP and various ICMP protocols for troubleshooting.

**Step 1:** Enable the interface, select VRF and enable DHCP.

The DMVPN design uses FVRF, so this interface must be placed into the VRF configured in the previous procedure.

```
interface GigabitEthernet0/0
  ip vrf forwarding INET-PUBLIC1
  ip address dhcp
  no cdp enable
  no shutdown
```

Do not enable PIM on this interface because no multicast traffic should be requested from this interface.

**Step 2:** Configure and apply the access list.

The IP access list must permit the protocols specified in the following table. The access list is applied inbound on the WAN interface, so filtering is done on traffic destined to the router.

Table 19 - Required DMVPN protocols

Name	Protocol	Usage
non500-isakmp	UDP 4500	IPsec via NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec
bootpc	UDP 68	DHCP

### Example

```
interface GigabitEthernet0/0
  ip access-group ACL-INET-PUBLIC in
  ip access-list extended ACL-INET-PUBLIC
  permit udp any any eq non500-isakmp
  permit udp any any eq isakmp
  permit esp any any
  permit udp any any eq bootpc
```

The additional protocols listed in the following table may assist in troubleshooting, but are not explicitly required to allow DMVPN to function properly.

Table 20 - Optional protocols-DMVPN spoke router

Name	Protocol	Usage
icmp echo	ICMP Type 0, Code 0	Allow remote pings
icmp echo-reply	ICMP Type 8, Code 0	Allow ping replies (from our requests)
icmp ttl-exceeded	ICMP Type 11, Code 0	Allow traceroute replies (from our requests)
icmp port-unreachable	ICMP Type 3, Code 3	Allow traceroute replies (from our requests)
UDP high ports	UDP > 1023, TTL=1	Allow remote traceroute

The additional optional entries for an access list to support ping are as follows:

```
permit icmp any any echo
permit icmp any any echo-reply
```

The additional optional entries for an access list to support traceroute are as follows:

```
permit icmp any any ttl-exceeded      ! for traceroute (sourced)
permit icmp any any port-unreachable  ! for traceroute (sourced)
permit udp any any gt 1023 ttl eq 1   ! for traceroute (destination)
```

## Procedure 4 Configure ISAKMP and IPsec

**Step 1:** Configure the crypto keyring.

The crypto keyring defines a PSK (or password) valid for IP sources reachable within a particular VRF. This key is a wildcard pre-shared key if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

**Step 2:** Configure the ISAKMP Policy and Dead Peer Detection.

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Standard (SHA)
- Authentication by PSK
- Diffie-Hellman group: 2

DPD is enabled with keepalive intervals sent at 30-second intervals with a 5-second retry interval, which is considered to be a reasonable setting to detect a failed hub.

```
crypto isakmp policy 10
encr aes 256
hash sha
authentication pre-share
group 2
!
crypto isakmp keepalive 30 5
```

**Step 3:** Create the ISAKMP profile.

The ISAKMP profile creates an association between an identity address, a VRF and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
keyring DMVPN-KEYRING1
match identity address 0.0.0.0 INET-PUBLIC1
```

**Step 4:** Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Since the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
mode transport
```

**Step 5:** Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE1
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
```

## Procedure 5 > Configure the mGRE Tunnel

**Step 1:** Configure basic interface settings.

Tunnel interfaces are created as they are configured. The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

The bandwidth setting should be set to match the Internet bandwidth.

Configure the IP MTU to 1400 and the **ip tcp adjust-mss** to 1360. There is a 40 byte difference, which corresponds to the combined IP and TCP header length.

```
interface Tunnel10
bandwidth [bandwidth (kbps)]
ip address [IP address] [netmask]
no ip redirects
ip mtu 1400
ip tcp adjust-mss 1360
```

**Step 2:** Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. The source interface should be the same interface used in to connect to the Internet. The **tunnel vrf** command should be set to the VRF defined previously for FVRF.

Enabling encryption on this interface requires the application of the IPsec profile configured in the previous procedure.

```
interface Tunnel10
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
 tunnel protection ipsec profile DMVPN-PROFILE1
```

### Step 3: Configure NHRP.

The DMVPN hub router is the NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.

The spoke router requires several additional configuration statements to define the NHRP server (NHS) and NHRP map statements for the DMVPN hub router mGRE tunnel IP address. EIGRP (configured in the following Procedure 6) relies on a multicast transport. Spoke routers require the NHRP static multicast mapping.

The value used for the NHS is the mGRE tunnel address for the DMVPN hub router. The map entries must be set to the outside NAT value of the DMVPN hub, as configured on the Cisco ASA5500. This design uses the values shown in Table 21.

Table 21 - DMVPN tunnel parameters

	Parameter value
DMVPN cloud	Primary
VRF	INET-PUBLIC1
DMVPN hub public address (actual)	192.168.18.10
DMVPN hub public address (externally routable after NAT)	172.16.130.1
Tunnel IP address (NHS)	10.4.34.1
Tunnel number	10
NHRP network ID	101

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. The NHRP cache holdtime should be configured to 600 seconds.

This design supports DMVPN spoke routers that receive their external IP addresses through DHCP. It is possible for these routers to acquire different IP addresses after a reload. When the router attempts to register with the NHRP server, it may appear as a duplicate to an entry already in the cache and be rejected. The **registration no-unique** option allows you to overwrite existing cache entries. This feature is only required on NHRP clients (DMVPN spoke routers).

The **ip nhrp redirect** command allows the DMVPN hub to notify spoke routers that a more optimal path may exist to a destination network, which may be required for DMVPN spoke-to-spoke direct communications. DMVPN spoke routers also use shortcut switching when building spoke-to-spoke tunnels.

```
interface Tunnel10
  ip nhrp authentication cisco123
  ip nhrp map 10.4.34.1 172.16.130.1
  ip nhrp map multicast 172.16.130.1
  ip nhrp network-id 101
  ip nhrp holdtime 600
  ip nhrp nhs 10.4.34.1
  ip nhrp registration no-unique
  ip nhrp shortcut
  ip nhrp redirect
```

#### Step 4: Configure EIGRP.

You configure EIGRP in the following procedure, but you need to configure some specific requirements for the mGRE tunnel interface first.

The EIGRP hello interval is increased to 20 seconds and the EIGRP hold time is increased to 60 seconds to accommodate up to 500 remote sites on a single DMVPN cloud.

```
interface Tunnel10
  ip hello-interval eigrp 200 20
  ip hold-time eigrp 200 60
```

The remote-site LAN networks must be advertised. The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. The summary address as configured below suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the DMVPN hub, which offers a measure of resiliency. If the various LAN networks cannot be summarized, then EIGRP continues to advertise the specific routes.

```
interface Tunnel10
  ip summary-address eigrp 200 [summary network] [summary mask]
```

### Procedure 6 Configure EIGRP

A single EIGRP process runs on the DMVPN spoke router. All interfaces on the router are EIGRP interfaces, but only the DMVPN tunnel interface is non-passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. All DMVPN spoke routers should run EIGRP stub routing to improve network stability and reduce resource utilization.

```
router eigrp 200
  network 10.4.34.0 0.0.1.255
  network 10.5.0.0 0.0.255.255
  network 10.255.0.0 0.0.255.255
  passive-interface default
  no passive-interface Tunnel10
  eigrp router-id [IP address of Loopback0]
  eigrp stub connected summary
  no auto-summary
```

## Procedure 7 Configure IP Multicast Routing

This procedure includes additional steps for configuring IP Multicast for a DMVPN tunnel on a router with IP Multicast already enabled.

**Step 1:** Configure PIM on the DMVPN tunnel interface.

Enable IP PIM sparse mode on the DMVPN tunnel interface.

```
interface Tunnel10
 ip pim sparse-mode
```

**Step 2:** Enable PIM non-broadcast multiple access mode for the DMVPN tunnel.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This inability to directly exchange information can also cause problems when running IP Multicast.

To resolve the NBMA issue, you need to implement a method where each remote PIM neighbor has its join messages tracked separately. A router in PIM NBMA mode treats each remote PIM neighbor as if it were connected to the router through a point-to-point link.

```
interface Tunnel10
 ip pim nbma-mode
```

**Step 3:** Configure the DR priority for the DMVPN spoke router.

Proper multicast operation across a DMVPN cloud requires that the hub router assumes the role of PIM Designated Router (DR). Spoke routers should never become the DR. You can prevent that by setting the DR priority to 0 for the spokes.

```
interface Tunnel10
 ip pim dr-priority 0
```

## Procedure 8 Connect Router to Access Layer Switch



### Reader Tip

Please refer to the [Campus Wired LAN Technology Design Guide](#) for complete access layer configuration details. This guide only includes the additional steps to complete the access layer configuration.

If you are using a remote-site distribution layer then skip to the “Deploying a WAN Remote-Site Distribution Layer” section of this guide.

Layer 2 EtherChannels are used to interconnect the CE router to the access layer in the most resilient method possible. If your access layer device is a single fixed configuration switch a simple Layer 2 trunk between the router and switch is used.

In the access layer design, the remote sites use collapsed routing, with 802.1Q trunk interfaces to the LAN access layer. The VLAN numbering is locally significant only.

## Option 1: Layer 2 EtherChannel from router to access layer switch

**Step 1:** Configure port-channel interface on the router.

```
interface Port-channel1
  description EtherChannel link to RS232-A2960S
  no shutdown
```

**Step 2:** Configure EtherChannel member interfaces on the router.

Configure the physical interfaces to tie to the logical port-channel using the channel-group command. The number for the port-channel and channel-group must match. Not all router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet0/1
  description RS232-A2960S Gig1/0/24
  !
interface GigabitEthernet0/2
  description RS232-A2960S Gig2/0/24
  !
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

**Step 3:** Configure EtherChannel member interfaces on the access layer switch.

Connect the router EtherChannel uplinks to separate switches in the access layer switch stack, or in the case of the Cisco Catalyst 4507R+E distribution layer, to separate redundant modules for additional resiliency.

The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration and reduces errors because most of the commands entered to a port-channel interface are copied to its members interfaces and do not require manual replication.

Configure two physical interfaces to be members of the EtherChannel. Also, apply the egress QoS macro that was defined in the LAN switch platform configuration procedure to ensure traffic is prioritized appropriately.

Not all connected router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet1/0/24
  description Link to RS232-2911-1 Gig0/1
interface GigabitEthernet2/0/24
  description Link to RS232-2911-1 Gig0/2
  !
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
  switchport
  macro apply EgressQoS
  channel-group 1 mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

**Step 4:** Configure EtherChannel trunk on the access layer switch.

An 802.1Q trunk is used which allows the router to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access layer switch. When using EtherChannel the interface type will be port-channel and the number must match the channel group configured in Step 3. DHCP Snooping and Address Resolution Protocol (ARP) inspection are set to trust.

```
interface Port-channel1
  description EtherChannel link to RS232-2911-1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,69
  switchport mode trunk
  ip arp inspection trust
  spanning-tree portfast trunk
  ip dhcp snooping trust
  no shutdown
```

The Catalyst 2960-S and 4500 do not require the **switchport trunk encapsulation dot1q** command.

## Option 2: Layer 2 trunk from router to access layer switch

**Step 1:** Enable the physical interface on the router.

```
interface GigabitEthernet0/2
  description RS231-A2960S Gig1/0/24
  no ip address
  no shutdown
```

**Step 2:** Configure the trunk on the access layer switch.

Use an 802.1Q trunk for the connection, which allows the router to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. DHCP Snooping and Address Resolution Protocol (ARP) inspection are set to trust.

```
interface GigabitEthernet1/0/24
  description Link to RS231-2911 Gig0/2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,69
  switchport mode trunk
  ip arp inspection trust
  spanning-tree portfast trunk
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  ip dhcp snooping trust
  no shutdown
```

The Catalyst 2960-S and 4500 do not require the **switchport trunk encapsulation dot1q** command.

## Procedure 9 Configure Access Layer Routing

**Step 1:** Create subinterfaces and assign VLAN tags.

After the physical interface or port-channel has been enabled, then the appropriate data or voice subinterfaces can be mapped to the VLANs on the LAN switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration. The subinterface portion of the configuration should be repeated for all data or voice VLANs.

```
interface [type] [number]. [sub-interface number]
  encapsulation dot1q [dot1q VLAN tag]
```

**Step 2:** Configure IP settings for each subinterface.

This design uses an IP addressing convention with the default gateway router assigned an IP address and IP mask combination of **N.N.N.1 255.255.255.0** where N.N.N is the IP network and 1 is the IP host.

When you are using a centralized DHCP server, your routers with LAN interfaces connected to a LAN using DHCP for end-station IP addressing must use an IP helper.

If the remote-site router is the first router of a dual-router design, then HSRP is configured at the access layer. This requires a modified IP configuration on each subinterface.

```
interface [type] [number]. [sub-interface number]
  ip address [LAN network 1] [LAN network 1 netmask]
  ip helper-address 10.4.48.10
  ip pim sparse-mode
```

### Example: Layer 2 EtherChannel

```
interface Port-channel1
  no ip address
  no shutdown
  !
  interface Port-channel1.64
  description Data
  encapsulation dot1q 64
  ip address 10.5.212.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
  !
  interface Port-channel1.69
  description Voice
  encapsulation dot1q 69
  ip address 10.5.213.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
```

## Example: Layer 2 Link

```
interface GigabitEthernet0/2
  no ip address
  no shutdown
!
interface GigabitEthernet0/2.64
  description Data
  encapsulation dot1Q 64
  ip address 10.5.192.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface GigabitEthernet0/2.69
  description Voice
  encapsulation dot1Q 69
  ip address 10.5.193.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
```

### PROCESS

## Enabling DMVPN Backup on a Remote Site Router

1. Configure VRF Lite
2. Connect to the Internet
3. Configure ISAKMP and IPsec
4. Configure the mGRE Tunnel
5. Configure EIGRP
6. Configure IP Multicast Routing
7. Control Usage of VPN with Static Routing

Use this set of procedures for any of the following topologies: DMVPN + DMVPN remote site, MPLS + DMVPN remote site, or Layer 2 WAN + DMVPN remote site.

This set of procedures includes the additional steps necessary to add a DMVPN backup link to a remote-site router that has already been configured with a primary WAN link using one of the following processes.

In this guide:

- Remote-Site DMVPN Spoke Router Configuration

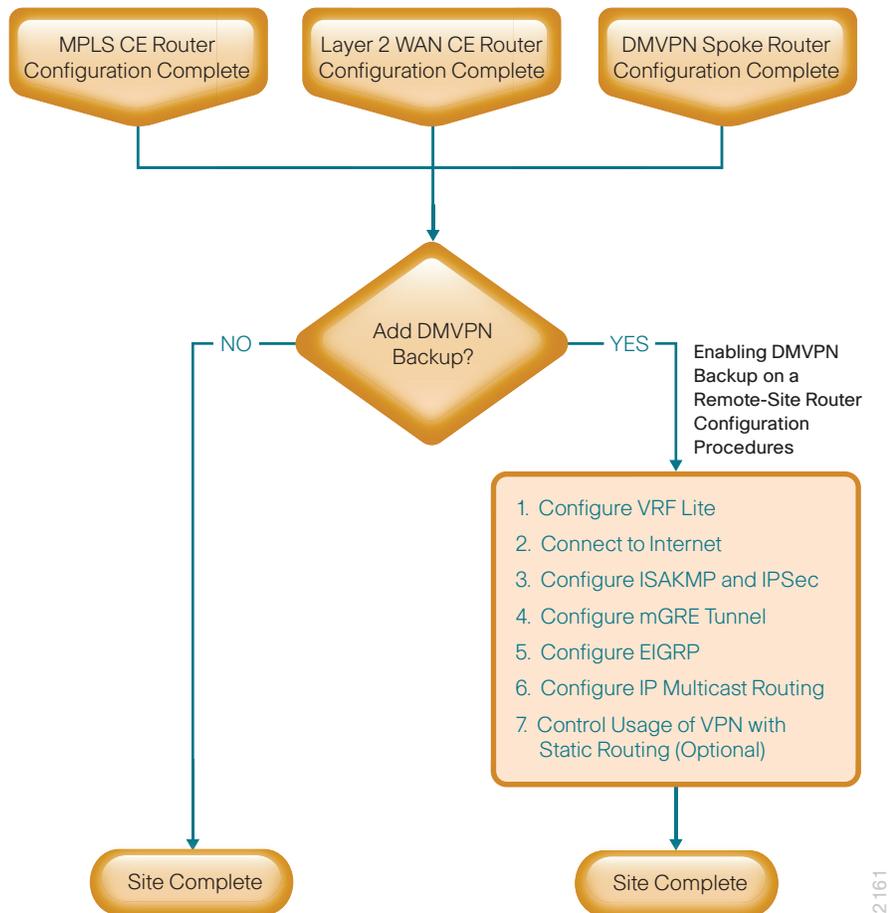
Or in these other guides:

- [MPLS WAN Technology Design Guide](#)—Remote-Site MPLS CE Router Configuration
- [Layer 2 WAN Technology Design Guide](#)—Remote-Site Layer 2 WAN CE Router Configuration

Only the additional procedures to add the DMVPN backup to the running remote-site router are included here.

The following flowchart provides details about how to add DMVPN backup on an existing remote-site router.

Figure 24 - Adding DMVPN Backup Configuration Flowchart



### Procedure 1 Configure VRF Lite

An Internet-facing VRF is created to support Front Door VRF for DMVPN. The VRF name is arbitrary but it is useful to select a name that describes the VRF. An associated RD must also be configured to make the VRF functional. The RD configuration also creates the routing and forwarding tables and associates the RD with the VRF instance.

This design uses VRF Lite so that the RD value can be chosen arbitrarily. It is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

When adding DMVPN backup to an already configured DMVPN spoke router, use a new VRF and other associated parameters as shown in the following table.

Table 22 - VRF Parameters for dual DMVPN

Parameter	Primary DMVPN cloud	Secondary DMVPN cloud
vrf	INET-PUBLIC1	INET-PUBLIC2
rd	65512:1	65512:2
crypto keyring	DMVPN-KEYRING1	DMVPN-KEYRING2
crypto isakmp profile	FVRF-ISAKMP-INET-PUBLIC1	FVRF-ISAKMP-INET-PUBLIC2
crypto ipsec profile	DMVPN-PROFILE1	DMVPN-PROFILE2

```
ip vrf INET-PUBLIC1
rd 65512:1
```

### Tech Tip

Command Reference:

An RD is either ASN-related (composed of an ASN and an arbitrary number) or IP-address-related (composed of an IP address and an arbitrary number).

You can enter an RD in either of these formats:

*16-bit autonomous-system-number:your 32-bit number*

For example, 65512:1.

*32-bit IP address: your 16-bit number*

For example, 192.168.122.15:1.

## Procedure 2 Connect to the Internet

The remote sites that are using DMVPN can use either static or dynamically assigned IP addresses. Cisco tested the design with a DHCP assigned external address, which also provides a dynamically configured default route.

The DMVPN spoke router connects directly to the Internet without a separate firewall. This connection is secured in two ways. Because the Internet interface is in a separate VRF, no traffic can access the global VRF except traffic sourced through the DMVPN tunnel. This design provides implicit security. Additionally, an IP access list permits only the traffic required for an encrypted tunnel, as well as DHCP and various ICMP protocols for troubleshooting.

**Step 1:** Enable the interface, select VRF and enable DHCP.

The DMVPN design uses FVRF, so this interface must be placed into the VRF configured in the previous procedure.

```
interface GigabitEthernet0/1
  ip vrf forwarding INET-PUBLIC1
  ip address dhcp
  no cdp enable
  no shutdown
```

**Step 2:** Configure and apply the access list.

The IP access list must permit the protocols specified in the following table. The access list is applied inbound on the WAN interface, so filtering is done on traffic destined to the router.

Table 23 - Required DMVPN protocols

Name	Protocol	Usage
non500-isakmp	UDP 4500	IPsec via NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec
bootpc	UDP 68	DHCP

## Example

```
interface GigabitEthernet0/1
  ip access-group ACL-INET-PUBLIC in
  ip access-list extended ACL-INET-PUBLIC
  permit udp any any eq non500-isakmp
  permit udp any any eq isakmp
  permit esp any any
  permit udp any any eq bootpc
```

The additional protocols listed in the following table may assist in troubleshooting, but are not explicitly required to allow DMVPN to function properly.

Table 24 - Optional protocols-DMVPN spoke router

Name	Protocol	Usage
icmp echo	ICMP Type 0, Code 0	Allow remote pings
icmp echo-reply	ICMP Type 8, Code 0	Allow ping replies (from our requests)
icmp ttl-exceeded	ICMP Type 11, Code 0	Allow traceroute replies (from our requests)
icmp port-unreachable	ICMP Type 3, Code 3	Allow traceroute replies (from our requests)
UDP high ports	UDP > 1023, TTL=1	Allow remote traceroute

The additional optional entries for an access list to support ping are as follows:

```
permit icmp any any echo
permit icmp any any echo-reply
```

The additional optional entries for an access list to support traceroute are as follows:

```
permit icmp any any ttl-exceeded      ! for traceroute (sourced)
permit icmp any any port-unreachable  ! for traceroute (sourced)
permit udp any any gt 1023 ttl eq 1   ! for traceroute (destination)
```

### Procedure 3 Configure ISAKMP and IPsec

**Step 1:** Configure the crypto keyring.

The crypto keyring defines a PSK (or password) valid for IP sources reachable within a particular VRF. This key is a wildcard PSK if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

**Step 2:** Configure the ISAKMP Policy and Dead Peer Detection.

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Standard (SHA)
- Authentication by PSK
- Diffie-Hellman group: 2

DPD is enabled with keepalive intervals sent at 30-second intervals with a 5-second retry interval, which is considered to be a reasonable setting to detect a failed hub.

```
crypto isakmp policy 10
encr aes 256
hash sha
authentication pre-share
group 2
!
crypto isakmp keepalive 30 5
```

**Step 3:** Create the ISAKMP profile.

The ISAKMP profile creates an association between an identity address, a VRF and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
keyring DMVPN-KEYRING1
match identity address 0.0.0.0 INET-PUBLIC1
```

**Step 4:** Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Since the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
mode transport
```

**Step 5:** Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE1
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
```

## Procedure 4 > Configure the mGRE Tunnel

**Step 1:** Configure basic interface settings.

Tunnel interfaces are created as they are configured. The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

The bandwidth setting should be set to match the Internet bandwidth.

Configure the IP MTU to 1400 and the **ip tcp adjust-mss** to 1360. There is a 40 byte difference, which corresponds to the combined IP and TCP header length.

```
interface Tunnel10
bandwidth [bandwidth (kbps)]
ip address [IP address] [netmask]
no ip redirects
ip mtu 1400
ip tcp adjust-mss 1360
```

**Step 2:** Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. Use the same source interface that you use to connect to the Internet. Set the **tunnel vrf** command should be set to the VRF defined previously for FVRF.

Enabling encryption on this interface requires the application of the IPsec profile configured in the previous procedure.

```
interface Tunnel10
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
 tunnel protection ipsec profile DMVPN-PROFILE1
```

### Step 3: Configure NHRP.

The DMVPN hub router is the NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.

The spoke router requires several additional configuration statements to define the NHRP server (NHS) and NHRP map statements for the DMVPN hub router mGRE tunnel IP address. EIGRP (configured in the following Procedure 5) relies on a multicast transport. Spoke routers require the NHRP static multicast mapping.

The value used for the NHS is the mGRE tunnel address for the DMVPN hub router. The map entries must be set to the outside NAT value of the DMVPN hub, as configured on the Cisco ASA5500. This design uses the values shown in Table 25.

Table 25 - DMVPN tunnel parameters

	Parameter values	
DMVPN cloud	Primary	Secondary
VRF	INET-PUBLIC1	INET-PUBLIC2
DMVPN hub public address (actual)	192.168.18.10	192.168.18.11
DMVPN hub public address (externally routable after NAT)	172.16.130.1	172.17.130.1
Tunnel IP address (NHS)	10.4.34.1	10.4.36.1
Tunnel number	10	11
NHRP network ID	101	102

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. The NHRP cache holdtime should be configured to 600 seconds.

This design supports DMVPN spoke routers that receive their external IP addresses through DHCP. It is possible for these routers to acquire different IP addresses after a reload. When the router attempts to register with the NHRP server, it may appear as a duplicate to an entry already in the cache and be rejected. The **registration no-unique** option allows you to overwrite existing cache entries. This feature is only required on NHRP clients (DMVPN spoke routers).

The **ip nhrp redirect** command allows the DMVPN hub to notify spoke routers that a more optimal path may exist to a destination network, which may be required for DMVPN spoke-to-spoke direct communications. DMVPN spoke routers also use shortcut switching when building spoke-to-spoke tunnels.

```
interface Tunnel10
  ip nhrp authentication cisco123
  ip nhrp map 10.4.34.1 172.16.130.1
  ip nhrp map multicast 172.16.130.1
  ip nhrp network-id 101
  ip nhrp holdtime 600
  ip nhrp nhs 10.4.34.1
  ip nhrp registration no-unique
  ip nhrp shortcut
  ip nhrp redirect
```

#### Step 4: Configure EIGRP.

You configure EIGRP is configured in the next procedure, but there are some specific requirements for the mGRE tunnel interface that you need to configure first.

The EIGRP hello interval is increased to 20 seconds and the EIGRP hold time is increased to 60 seconds to accommodate up to 500 remote sites on a single DMVPN cloud.

```
interface Tunnel10
  ip hello-interval eigrp 200 20
  ip hold-time eigrp 200 60
```

The remote-site LAN networks must be advertised. The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. The summary address as configured below suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the DMVPN hub, which offers a measure of resiliency. If the various LAN networks cannot be summarized, EIGRP continues to advertise the specific routes.

```
interface Tunnel10
  ip summary-address eigrp 200 [summary network] [summary mask]
```

### Procedure 5 Configure EIGRP

An additional EIGRP-200 process runs on the DMVPN spoke router for the second DMVPN cloud. All interfaces on the router are EIGRP interfaces, but only the DMVPN tunnel interface is non-passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. All DMVPN spoke routers should run EIGRP stub routing to improve network stability and reduce resource utilization.

```
router eigrp 200
  network 10.4.34.0 0.0.1.255
  network 10.5.0.0 0.0.255.255
  network 10.255.0.0 0.0.255.255
  passive-interface default
  no passive-interface Tunnel10
  eigrp router-id [IP address of Loopback0]
  eigrp stub connected summary
  no auto-summary
```

## Procedure 6 Configure IP Multicast Routing

This procedure includes additional steps for configuring IP Multicast for a DMVPN tunnel on a router with IP Multicast already enabled.

**Step 1:** Configure PIM on the DMVPN tunnel interface.

Enable IP PIM sparse mode on the DMVPN tunnel interface.

```
interface Tunnel10
  ip pim sparse-mode
```

**Step 2:** Enable PIM NBMA mode for the DMVPN tunnel.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This inability to directly exchange information can also cause problems when running IP Multicast.

To resolve the NBMA issue, you need to implement a method where each remote PIM neighbor has its join messages tracked separately. A router in PIM NBMA mode treats each remote PIM neighbor as if it were connected to the router through a point-to-point link.

```
interface Tunnel10
  ip pim nbma-mode
```

**Step 3:** Configure the DR priority for the DMVPN spoke router.

Proper multicast operation across a DMVPN cloud requires that the hub router assumes the role of PIM Designated Router (DR). Spoke routers should never become the DR. You can prevent that by setting the DR priority to 0 for the spokes.

```
interface Tunnel10
  ip pim dr-priority 0
```

## Procedure 7 Control Usage of VPN with Static Routing

This procedure is optional, and is only required when using an MPLS WAN with static routing.

This procedure should be used to control the VPN usage for the dual-link designs (single-router, dual-link) when adding VPN backup and static routing with the service provider is used. The MPLS VPN is the primary WAN transport, and as long as it is operational, the tunnel interface remains shut down.

The remote-site router can use the IP SLA feature to send echo probes to the site's MPLS PE router, and if the PE router becomes unreachable, then the router can use the Embedded Event Manager (EEM) to dynamically enable the tunnel interface.

**Step 1:** Enable the IP SLA probe.

Standard ICMP echo (ping) probes are used and are sent at 15-second intervals. Responses must be received before the timeout of 1000 ms expires. If using the MPLS PE router as the probe destination, the destination address is the same as the static route next hop address already configured. Use the MPLS WAN interface as the probe source-interface.

```
ip sla [probe number]
  icmp-echo [probe destination IP address] source-interface [interface]
  timeout 1000
  threshold 1000
  frequency 15
ip sla schedule [probe number] life forever start-time now
```

**Step 2:** Configure Enhanced Object Tracking.

This step links the status of the IP SLA probe to an object which is monitored by EEM scripts.

```
track [object number] ip sla [probe number] reachability
```

**Step 3:** Configure EEM scripting to enable or disable the tunnel interface.

An event-tracking EEM script monitors the state of an object and runs router IOS commands for that particular state. It is also a best practice to generate syslog messages that provide status information regarding EEM.

```
event manager applet [EEM script name]
  event track [object number] state [tracked object state]
  action [sequence 1] cli command "[command 1]"
  action [sequence 2] cli command "[command 2]"
  action [sequence 3] cli command "[command 3]"
  action [sequence ...] cli command "[command ...]"
  action [sequence N] syslog msg "[syslog message test]"
```

### Example

```
track 60 ip sla 200 reachability
ip sla 200
  icmp-echo 192.168.6.142 source-interface GigabitEthernet0/0
  threshold 1000
  frequency 15
ip sla schedule 200 life forever start-time now
```

EEM script to enable tunnel interface upon MPLS link failure:

```
event manager applet ACTIVATE-VPN
  event track 60 state down
  action 1 cli command "enable"
  action 2 cli command "configure terminal"
  action 3 cli command "interface tunnel10"
  action 4 cli command "no shutdown"
  action 5 cli command "end"
  action 99 syslog msg "Primary Link Down - Activating VPN interface"
```

EEM script to disable tunnel interface upon MPLS link restoration:

```
event manager applet DEACTIVATE-VPN
  event track 60 state up
  action 1 cli command "enable"
  action 2 cli command "configure terminal"
  action 3 cli command "interface tunnel10"
  action 4 cli command "shutdown"
  action 5 cli command "end"
  action 99 syslog msg "Primary Link Restored - Deactivating VPN interface"
```

## PROCESS

### Router 1 Modifications for Dual Router Design

1. Configure Access Layer HSRP
2. Configure Transit Network
3. Configure EIGRP (LAN Side)
4. Enable Enhanced Object Tracking
5. Configure Loopback Resiliency

This process is required when the first router has already been configured using one of the following processes.

In this guide:

- [Remote-Site DMVPN Spoke Router Configuration](#)

Or in these other guides:

- [MPLS WAN Technology Design Guide](#)—Remote-Site MPLS CE Router Configuration
- [Layer 2 WAN Technology Design Guide](#)—Remote-Site Layer 2 WAN CE Router Configuration

### Procedure 1 Configure Access Layer HSRP

You need to configure HSRP to enable the use of a Virtual IP (VIP) as a default gateway that is shared between two routers. The HSRP active router is the router connected to the primary carrier and the HSRP standby router is the router connected to the secondary carrier or backup link. Configure the HSRP active router with a standby priority that is higher than the HSRP standby router.

The router with the higher standby priority value is elected as the HSRP active router. The preempt option allows a router with a higher priority to become the HSRP active, without waiting for a scenario where there is no router in the HSRP active state. The relevant HSRP parameters for the router configuration are shown in the following table.

Table 26 - WAN remote-site HSRP parameters (dual router)

Router	HSRP role	Virtual IP address (VIP)	Real IP address	HSRP priority	PIM DR priority
Primary	Active	.1	.2	110	110
Secondary	Standby	.1	.3	105	105

The assigned IP addresses override those configured in the previous procedure, so the default gateway IP address remains consistent across locations with single or dual routers.

The dual-router access-layer design requires a modification for resilient multicast. The PIM designated router (DR) should be on the HSRP active router. The DR is normally elected based on the highest IP address, and has no awareness of the HSRP configuration. In this design, the HSRP active router has a lower real IP address than the HSRP standby router, which requires a modification to the PIM configuration. The PIM DR election can be influenced by explicitly setting the DR priority on the LAN-facing subinterfaces for the routers.



### Tech Tip

The HSRP priority and PIM DR priority are shown in the previous table to be the same value; however you are not required to use identical values.

This procedure should be repeated for all data or voice subinterfaces.

```
interface [type] [number]. [sub-interface number]
  encapsulation dot1Q [dot1q VLAN tag]
  ip address [LAN network 1 address] [LAN network 1 netmask]
  ip helper-address 10.4.48.10
  ip pim sparse-mode
  ip pim dr-priority 110
  standby version 2
  standby 1 ip [LAN network 1 gateway address]
  standby 1 priority 110
  standby 1 preempt
  standby 1 authentication md5 key-string cisco123
```

### Example: Layer 2 Link

```
interface GigabitEthernet0/2
  no ip address
  no shutdown
!
interface GigabitEthernet0/2.64
  description Data
  encapsulation dot1Q 64
  ip address 10.5.212.2 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim dr-priority 110
  ip pim sparse-mode
  standby version 2
  standby 1 ip 10.5.212.1
  standby 1 priority 110
  standby 1 preempt
  standby 1 authentication md5 key-string cisco123
!
interface GigabitEthernet0/2.69
  description Voice
```

```

encapsulation dot1Q 69
ip address 10.5.213.2 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 110
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.213.1
standby 1 priority 110
standby 1 preempt
standby 1 authentication md5 key-string cisco123

```

## Procedure 2 Configure Transit Network

The transit network is configured between the two routers. This network is used for router-router communication and to avoid hair-pinning. The transit network should use an additional subinterface on the router interface that is already being used for data or voice.

There are no end stations connected to this network, so HSRP and DHCP are not required.

```

interface [type][number].[sub-interface number]
  encapsulation dot1Q [dot1q VLAN tag]
  ip address [transit net address] [transit net netmask]
  ip pim sparse-mode

```

### Example

```

interface GigabitEthernet0/2.99
  description Transit Net
  encapsulation dot1Q 99
  ip address 10.5.208.1 255.255.255.252
  ip pim sparse-mode

```

**Step 1:** Add transit network VLAN to the access layer switch.

If the VLAN does not already exist on the access layer switch, configure it now.

```

vlan 99
  name Transit-net

```

**Step 2:** Add transit network VLAN to existing access layer switch trunk.

```

interface GigabitEthernet1/0/24
  switchport trunk allowed vlan add 99

```

### Procedure 3 Configure EIGRP (LAN Side)

You must configure a routing protocol between the two routers. This ensures that the HSRP active router has full reachability information for all WAN remote sites.

#### Step 1: Enable EIGRP-100.

Configure EIGRP-100 facing the access layer. In this design, all LAN-facing interfaces and the loopback must be EIGRP interfaces. All interfaces except the transit-network subinterface should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. Do not include the DMVPN mGRE interface as an EIGRP-100 interface.

```
router eigrp 100
  network [network] [inverse mask]
  passive-interface default
  no passive-interface [Transit interface]
  eigrp router-id [IP address of Loopback0]
  no auto-summary
```

#### Step 2: Redistribute WAN routing protocol into EIGRP-100.

The remote-site router is using either BGP for an MPLS connection or EIGRP for a Layer 2 WAN or DMVPN connection. The WAN-facing routing protocol in use needs to be distributed into the EIGRP-100.

EIGRP-200 or EIGRP-300 are already configured in a DMVPN or Layer 2 WAN deployment, and routes from these EIGRP processes are redistributed. Since the routing protocol is the same, no default metric is required.

```
router eigrp 100
  redistribute eigrp 200
```

BGP is already configured for a MPLS deployment. The BGP routes are redistributed into EIGRP with a default metric. By default, only the WAN bandwidth and delay values are used for metric calculation.

```
router eigrp 100
  default-metric [WAN bandwidth] [WAN delay] 255 1 1500
  redistribute bgp 65511
```

#### Example: EIGRP into EIGRP

```
router eigrp 100
  network 10.4.0.0 0.1.255.255
  network 10.255.0.0 0.0.255.255
  redistribute eigrp 200
  passive-interface default
  no passive-interface GigabitEthernet0/2.99
  eigrp router-id 10.255.253.232
  no auto-summary
```

### Example: BGP into EIGRP

```
router eigrp 100
  default-metric 100000 100 255 1 1500
  network 10.4.0.0 0.1.255.255
  network 10.255.0.0 0.0.255.255
  redistribute bgp 65511
  passive-interface default
  no passive-interface GigabitEthernet0/2.99
  eigrp router-id 10.255.252.206
  no auto-summary
```

### Procedure 4 Enable Enhanced Object Tracking

The HSRP active router remains the active router unless the router is reloaded or fails. Having the HSRP router remain as the active router can lead to undesired behavior. If the primary WAN transport were to fail, the HSRP active router would learn an alternate path through the transit network to the HSRP standby router and begin to forward traffic across the alternate path. This is sub-optimal routing, and you can address it by using EOT.

The HSRP active router (MPLS CE, Layer 2 WAN CE, or primary DMVPN spoke) can use the IP SLA feature to send echo probes to an upstream neighbor router and if that router becomes unreachable, then the router can lower its HSRP priority, so that the HSRP standby router can preempt and become the HSRP active router.

This procedure is valid only on the router connected to the primary transport.

#### Step 1: Enable the IP SLA probe.

Use standard ICMP echo (ping) probes, and send them at 15 second intervals. Responses must be received before the timeout of 1000 ms expires. If using the MPLS PE router as the probe destination, the destination address is the same as the BGP neighbor address. If using the Layer WAN CE router as the probe destination, then the destination address is either the CE router address when using the simple demarcation or the subinterface CE router address when using a trunked demarcation. If using the DMVPN hub router as the probe destination, then the destination address is the mGRE tunnel address.

```
ip sla 100
  icmp-echo [probe destination IP address] source-interface [WAN interface]
  timeout 1000
  threshold 1000
  frequency 15
  ip sla schedule 100 life forever start-time now
```

#### Step 2: Configure EOT.

A tracked object is created based on the IP SLA probe. The object being tracked is the reachability success or failure of the probe. If the probe is successful, the tracked object status is Up; if it fails, the tracked object status is Down.

```
track 50 ip sla 100 reachability
```

**Step 3:** Link HSRP with the tracked object.

All data or voice subinterfaces should enable HSRP tracking.

HSRP can monitor the tracked object status. If the status is down, the HSRP priority is decremented by the configured priority. If the decrease is large enough, the HSRP standby router preempts.

```
interface [interface type] [number].[sub-interface number]
  standby 1 track 50 decrement 10
```

### Example

```
ip sla 100
  icmp-echo 192.168.3.10 source-interface GigabitEthernet0/0
  timeout 1000
  threshold 1000
  frequency 15
ip sla schedule 100 life forever start-time now
!
track 50 ip sla 100 reachability
!
!
interface GigabitEthernet0/2.64
  standby 1 track 50 decrement 10
!
interface GigabitEthernet0/2.69
  standby 1 track 50 decrement 10
```

## Procedure 5 Configure Loopback Resiliency

The remote-site routers have in-band management configured via the loopback interface. To ensure reachability of the loopback interface in a dual-router design, redistribute the loopback of the adjacent router into the WAN routing protocol. The procedure varies depending on which WAN routing protocol is in use.

### Option 1: MPLS CE Router with BGP

**Step 1:** Configure BGP to advertise the adjacent router's loopback IP address.

```
router bgp 65511
  network 10.255.253.203 mask 255.255.255.255
```

### Option 2: DMVPN Spoke Router or Layer 2 WAN CE Router with EIGRP

**Step 1:** Configure an access list to limit the redistribution to only the adjacent router's loopback IP address.

```
ip access-list standard R[number]-LOOPBACK
  permit [IP Address of Adjacent Router Loopback]
!
route-map LOOPBACK-ONLY permit 10
  match ip address R[number]-LOOPBACK
```

### Example

```
ip access-list standard R2-LOOPBACK
 permit 10.255.253.211
!
route-map LOOPBACK-ONLY permit 10
 match ip address R2-LOOPBACK
```

**Step 2:** Configure EIGRP to redistribute the adjacent router's loopback IP address. The EIGRP stub routing must be adjusted to permit redistributed routes.

### Example: DMVPN Spoke Router

```
router eigrp 200
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp stub connected summary redistributed
```

### Example: Layer 2 WAN CE Router

```
router eigrp 300
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp stub connected summary redistributed
```

## Remote-Site DMVPN Spoke Router Configuration (Router 2)

1. Configure the WAN Remote Router
2. Configure VRF Lite
3. Connect to the Internet
4. Configure ISAKMP and IPsec
5. Configure the mGRE Tunnel
6. Configure EIGRP
7. Configure IP Multicast Routing
8. Connect Router to Access Layer Switch
9. Configure Access Layer Interfaces
10. Configure Access Layer HSRP
11. Configure Transit Network
12. Configure EIGRP (LAN Side)
13. Configure Loopback Resiliency

These procedures are used when you configure the second router of a dual-router, dual-link design for any of the following topologies: DMVPN + DMVPN remote site, MPLS + DMVPN remote site, or Layer 2 WAN + DMVPN remote site.

This set of procedures includes the additional steps necessary to configure a second router as a DMVPN spoke router when the first router has already been configured with the process Remote-Site DMVPN Spoke Router Configuration.

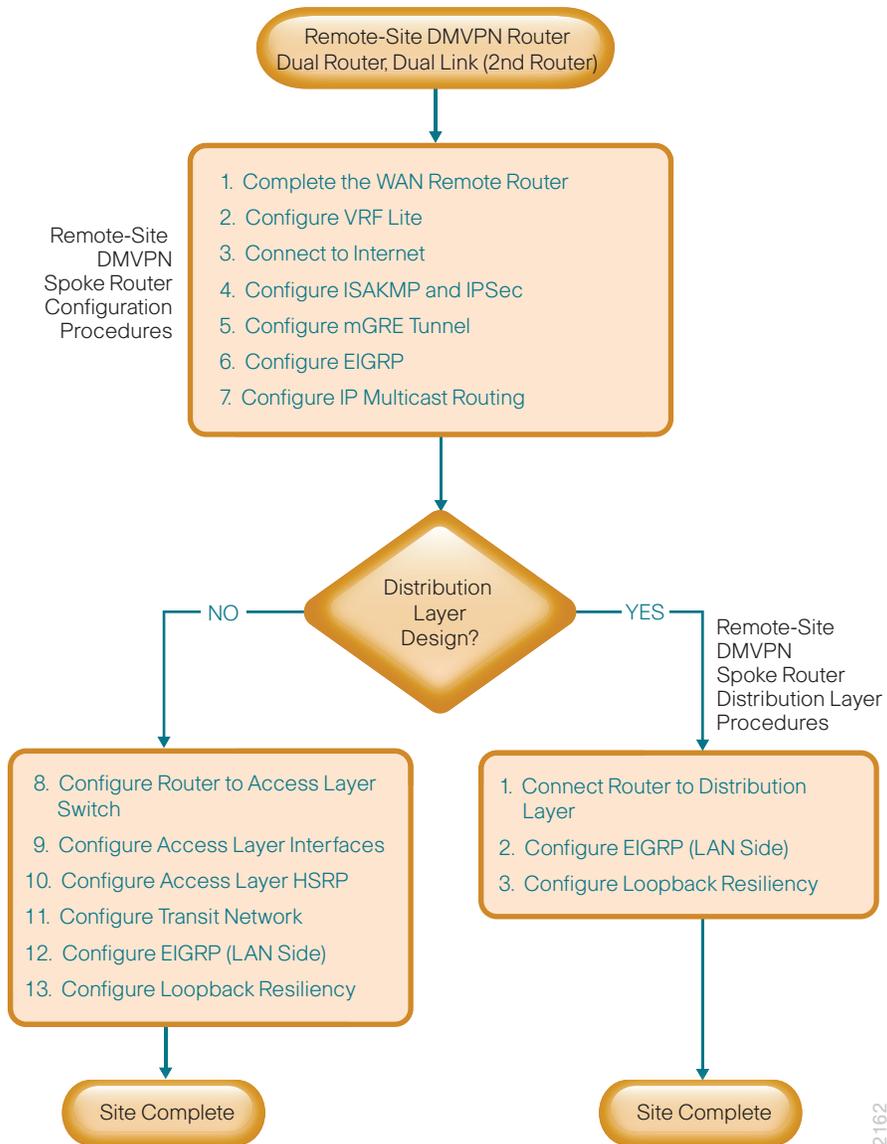
Alternatively, if the first router was configured using one of the following processes from a different CVD guide:

- [MPLS WAN Technology Design Guide](#)—Remote-Site MPLS CE Router Configuration
- [Layer 2 WAN Technology Design Guide](#)—Remote-Site Layer 2 WAN CE Router Configuration

Then the previous process, Router 1 Modifications for Dual Router Design, must also be completed.

The following flowchart provides details about how to complete the configuration of a remote-site DMVPN spoke router.

Figure 25 - Remote-site DMVPN spoke router configuration flowchart



## Procedure 1 Configure the WAN Remote Router

Within this design, there are features and services that are common across all WAN remote-site routers. These are system settings that simplify and secure the management of the solution.

**Step 1:** Configure the device host name to make it easy to identify the device.

```
hostname [hostname]
```

**Step 2:** Configure local login and password.

The local login account and password provides basic access authentication to a router which provides only limited operational privileges. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the disclosure of plain text passwords when viewing configuration files.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

**Step 3:** By default, https access to the router will use the enable password for authentication.

**Step 4:** (Optional) Configure centralized user authentication.

As networks scale in the number of devices to maintain it poses an operational burden to maintain local user accounts on every device. A centralized Authentication, Authorization and Accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
tacacs server TACACS-SERVER-1
  address ipv4 10.4.48.15
  key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

**Step 5:** Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the network device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

Specify the transport preferred none on vty lines to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
  transport preferred none
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
  logging synchronous
```

Enable Simple Network Management Protocol (SNMP) to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

**Step 6:** (Optional) In networks where network operational support is centralized you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```



### Tech Tip

If you configure an access-list on the vty interface you may lose the ability to use ssh to login from one router to the next for hop-by-hop troubleshooting.

**Step 7:** Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organizations network.

You should program network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

**Step 8:** Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from a unique network range that is not part of any other internal network summary range.

```
interface Loopback 0
 ip address [ip address] 255.255.255.255
 ip pim sparse-mode
```

The **ip pim sparse-mode** command will be explained further in the process.

Bind the device processes for SNMP, SSH, PIM, TACACS+ and NTP to the loopback interface address for optimal resiliency:

```
snmp-server trap-source Loopback0
ip ssh source-interface Loopback0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

**Step 9:** Configure IP Multicast routing.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a Broadcast stream that would propagate everywhere. IP Telephony MOH and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an IGMP message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as an RP to map the receivers to active sources so they can join their streams.

In this design, which is based on sparse mode multicast operation, Auto RP is used to provide a simple yet scalable way to provide a highly resilient RP environment.

Enable IP Multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

Every Layer 3 switch and router must be configured to discover the IP Multicast RP with `autorp`. Use the **ip pim autorp listener** command to allow for discovery across sparse mode links. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

```
ip pim sparse-mode
```

## Procedure 2 Configure VRF Lite

An Internet-facing VRF is created to support FVRF for DMVPN. The VRF name is arbitrary but it is useful to select a name that describes the VRF. You must also configure an associated RD to make the VRF functional. The RD configuration creates the routing and forwarding tables and associates the RD with the VRF instance.

This design uses VRF Lite so that the RD value can be chosen arbitrarily. It is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

When you are configuring a DMVPN link on a secondary DMVPN cloud, use a new VRF and other associated parameters as shown in the following table.

Table 27 - VRF Parameters for dual DMVPN

Parameter	Primary DMVPN cloud	Secondary DMVPN cloud
vrf	INET-PUBLIC1	INET-PUBLIC2
rd	65512:1	65512:2
tunnel number	10	11
crypto keyring	DMVPN-KEYRING1	DMVPN-KEYRING2
crypto isakmp profile	FVRF-ISAKMP-INET-PUBLIC1	FVRF-ISAKMP-INET-PUBLIC2
crypto ipsec profile	DMVPN-PROFILE1	DMVPN-PROFILE2

```
ip vrf INET-PUBLIC2  
rd 65512:2
```



## Tech Tip

Command Reference:

An RD is either ASN-related (composed of an ASN and an arbitrary number) or IP-address-related (composed of an IP address and an arbitrary number).

You can enter an RD in either of these formats:

*16-bit autonomous-system-number:your 32-bit number*

For example, 65512:1.

*32-bit IP address: your 16-bit number*

For example, 192.168.122.15:1.

## Procedure 3 Connect to the Internet

The remote sites using DMVPN can use either static or dynamically assigned IP addresses. We tested the design with a DHCP assigned external address, which also provides a dynamically configured default route.

The DMVPN spoke router connects directly to the Internet without a separate firewall. This connection is secured in two ways. Because the Internet interface is in a separate VRF, no traffic can access the global VRF except traffic sourced through the DMVPN tunnel. This design provides implicit security. Additionally, an IP access list permits only the traffic required for an encrypted tunnel, as well as DHCP and various ICMP protocols for troubleshooting.

**Step 1:** Enable the interface, select VRF and enable DHCP.

The DMVPN design uses FVRF, so this interface must be placed into the VRF configured in the previous procedure.

```
interface GigabitEthernet0/0
  ip vrf forwarding INET-PUBLIC2
  ip address dhcp
  no cdp enable
  no shutdown
```

Do not enable PIM on this interface because no multicast traffic should be requested from this interface.

**Step 2:** Configure and apply the access list.

The IP access list must permit the protocols specified in the following table. The access list is applied inbound on the WAN interface, so filtering is done on traffic destined to the router.

Table 28 - Required DMVPN protocols

Name	Protocol	Usage
non500-isakmp	UDP 4500	IPsec via NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec
bootpc	UDP 68	DHCP

### Example

```
interface GigabitEthernet0/0
 ip access-group ACL-INET-PUBLIC in
 ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
```

The additional protocols listed in the following table may assist in troubleshooting, but are not explicitly required to allow DMVPN to function properly.

Table 29 - Optional protocols-DMVPN spoke router

Name	Protocol	Usage
icmp echo	ICMP Type 0, Code 0	Allow remote pings
icmp echo-reply	ICMP Type 8, Code 0	Allow ping replies (from our requests)
icmp ttl-exceeded	ICMP Type 11, Code 0	Allow traceroute replies (from our requests)
icmp port-unreachable	ICMP Type 3, Code 3	Allow traceroute replies (from our requests)
UDP high ports	UDP > 1023, TTL=1	Allow remote traceroute

The additional optional entries for an access list to support ping are as follows:

```
permit icmp any any echo
permit icmp any any echo-reply
```

The additional optional entries for an access list to support traceroute are as follows:

```
permit icmp any any ttl-exceeded      ! for traceroute (sourced)
permit icmp any any port-unreachable  ! for traceroute (sourced)
permit udp any any gt 1023 ttl eq 1   ! for traceroute (destination)
```

## Procedure 4 Configure ISAKMP and IPsec

**Step 1:** Configure the crypto keyring.

The crypto keyring defines a PSK (or password) valid for IP sources reachable within a particular VRF. This key is a wildcard pre-shared key if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto keyring DMVPN-KEYRING2 vrf INET-PUBLIC2
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

**Step 2:** Configure the ISAKMP Policy and Dead Peer Detection (DPD).

The ISAKMP policy for DMVPN uses the following:

- Advanced Encryption Standard (AES) with a 256-bit key
- Secure Hash Standard (SHA)
- Authentication by PSK
- Diffie-Hellman group: 2

DPD is enabled with keepalive intervals sent at 30-second intervals with a 5-second retry interval, which is considered to be a reasonable setting to detect a failed hub.

```
crypto isakmp policy 10
  encr aes 256
  hash sha
  authentication pre-share
  group 2
!
crypto isakmp keepalive 30 5
```

**Step 3:** Create the ISAKMP profile.

The ISAKMP profile creates an association between an identity address, a VRF and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0.

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC2
  keyring DMVPN-KEYRING2
  match identity address 0.0.0.0 INET-PUBLIC2
```

**Step 4:** Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit AES encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Since the DMVPN hub router is behind a NAT device, you must configure the IPsec transform for transport mode.

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
  mode transport
```

**Step 5:** Create the IPsec profile.

The IPsec profile creates an association between an ISAKMP profile and an IPsec transform-set.

```
crypto ipsec profile DMVPN-PROFILE2
  set transform-set AES256/SHA/TRANSPORT
  set isakmp-profile FVRF-ISAKMP-INET-PUBLIC2
```

## Procedure 5 Configure the mGRE Tunnel

**Step 1:** Configure basic interface settings.

You create tunnel interfaces as you configure them. The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

The bandwidth setting should be set to match the Internet bandwidth.

The IP MTU should be configured to 1400 and the `ip tcp adjust-mss` should be configured to 1360. There is a 40 byte difference, which corresponds to the combined IP and TCP header length.

```
interface Tunnel11
  bandwidth [bandwidth (kbps)]
  ip address [IP address] [netmask]
  no ip redirects
  ip mtu 1400
  ip tcp adjust-mss 1360
```

**Step 2:** Configure the tunnel.

DMVPN uses multipoint GRE (mGRE) tunnels. This type of tunnel requires a source interface only. The source interface should be the same interface you use to connect to the Internet. You should set the `tunnel vrf` command to the VRF defined previously for FVRF.

To enable encryption on this interface, you must apply the IPsec profile that you configured in the previous procedure.

```
interface Tunnel11
  tunnel source GigabitEthernet0/0
  tunnel mode gre multipoint
  tunnel vrf INET-PUBLIC2
  tunnel protection ipsec profile DMVPN-PROFILE2
```

**Step 3:** Configure NHRP.

The DMVPN hub router is the NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.

The spoke router requires several additional configuration statements to define the NHRP server (NHS) and NHRP map statements for the DMVPN hub router mGRE tunnel IP address. EIGRP (configured in the following Procedure 6) relies on a multicast transport. Spoke routers require the NHRP static multicast mapping.

For the NHS value, use the mGRE tunnel address for the DMVPN hub router. The map entries must be set to the outside NAT value of the DMVPN hub, as configured on the Cisco ASA5500. This design uses the values shown in Table 30.

Table 30 - DMVPN tunnel parameters

	Parameter values	
	Primary	Secondary
DMVPN cloud	Primary	Secondary
VRF	INET-PUBLIC1	INET-PUBLIC2
DMVPN hub public address (externally routable after NAT)	172.16.130.1	172.17.130.1
Tunnel IP address	10.4.34.1/23	10.4.36.1/23
Tunnel number	10	11
NHRP network ID	101	102
EIGRP AS	200	201

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. You should configure the NHRP cache holdtime to 600 seconds.

This design supports DMVPN spoke routers that receive their external IP addresses through DHCP. It is possible for these routers to acquire different IP addresses after a reload. When the router attempts to register with the NHRP server, it may appear as a duplicate to an entry already in the cache and be rejected. The **registration no-unique** option allows you to overwrite existing cache entries. This feature is only required on NHRP clients (DMVPN spoke routers).

The **ip nhrp redirect** command allows the DMVPN hub to notify spoke routers that a more optimal path may exist to a destination network, which may be required for DMVPN spoke-to-spoke direct communications. DMVPN spoke routers also use shortcut switching when building spoke-to-spoke tunnels.

```
interface Tunnel11
 ip nhrp authentication cisco123
 ip nhrp map 10.4.36.1 172.17.130.1
 ip nhrp map multicast 172.17.130.1
 ip nhrp network-id 102
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.36.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
```

#### Step 4: Configure EIGRP.

You configure EIGRP in the next procedure, but you need to configure some specific requirements for the mGRE tunnel interface first.

Increase the EIGRP hello interval to 20 seconds and the EIGRP hold time to 60 seconds to accommodate up to 500 remote sites on a single DMVPN cloud.

```
interface Tunnel11
 ip hello-interval eigrp 201 20
 ip hold-time eigrp 201 60
```

You must advertise the remote-site LAN networks. The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. The summary address as configured below suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the DMVPN hub, which offers a measure of resiliency. If the various LAN networks cannot be summarized, then EIGRP continues to advertise the specific routes.

```
interface Tunnel11
 ip summary-address eigrp 201 [summary network] [summary mask]
```

## Procedure 6 Configure EIGRP

An additional EIGRP process (200 or 201) runs on the DMVPN spoke router for the associated DMVPN cloud. All interfaces on the router are EIGRP interfaces, but only the DMVPN tunnel interface is non-passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. All DMVPN spoke routers should run EIGRP stub routing to improve network stability and reduce resource utilization.

```
router eigrp 201
 network 10.4.36.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel11
 eigrp router-id [IP address of Loopback0]
 eigrp stub connected summary
 no auto-summary
```

## Procedure 7 Configure IP Multicast Routing

This procedure includes additional steps for configuring IP Multicast for a DMVPN tunnel on a router with IP Multicast already enabled.

**Step 1:** Configure PIM on the DMVPN tunnel interface.

Enable IP PIM sparse mode on the DMVPN tunnel interface.

```
interface Tunnel11
 ip pim sparse-mode
```

**Step 2:** Enable PIM NBMA mode for the DMVPN tunnel.

Spoke-to-spoke DMVPN networks present a unique challenge because the spokes cannot directly exchange information with one another, even though they are on the same logical network. This inability to directly exchange information can also cause problems when running IP Multicast.

To resolve the NBMA issue, you need to implement a method where each remote PIM neighbor has its join messages tracked separately. A router in PIM NBMA mode treats each remote PIM neighbor as if it were connected to the router through a point-to-point link.

```
interface Tunnel11
 ip pim nbma-mode
```

**Step 3:** Configure the DR priority for the DMVPN spoke router.

Proper multicast operation across a DMVPN cloud requires that the hub router assumes the role of PIM Designated Router (DR). Spoke routers should never become the DR. You can prevent that by setting the DR priority to 0 for the spokes.

```
interface Tunnel11
  ip pim dr-priority 0
```

## Procedure 8 Connect Router to Access Layer Switch



### Reader Tip

Please refer to the [Campus Wired LAN Technology Design Guide](#) for complete access layer configuration details. This guide only includes the additional steps to complete the access layer configuration.

If you are using a remote-site distribution layer then skip to the “Deploying a WAN Remote-Site Distribution Layer” section of this guide.

Layer 2 EtherChannels are used to interconnect the CE router to the access layer in the most resilient method possible, unless the access layer device is a single fixed configuration switch, otherwise a simple Layer 2 trunk between the router and switch is used.

In the access layer design, the remote sites use collapsed routing, with 802.1Q trunk interfaces to the LAN access layer. The VLAN numbering is locally significant only.

### Option 1: Layer 2 EtherChannel from router to access layer switch

**Step 1:** Configure port-channel interface on the router.

```
interface Port-channel2
  description EtherChannel link to RS232-A2960S
  no shutdown
```

**Step 2:** Configure EtherChannel member interfaces on the router.

Configure the physical interfaces to tie to the logical port-channel using the channel-group command. The number for the port-channel and channel-group must match. Not all router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet0/1
  description RS232-A2960S Gig1/0/23
  !
interface GigabitEthernet0/2
  description RS232-A2960S Gig2/0/23
  !
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 2
  no shutdown
```

**Step 3:** Configure EtherChannel member interfaces on the access layer switch.

Connect the router EtherChannel uplinks to separate switches in the access layer switch stack, or in the case of the Cisco Catalyst 4507R+E distribution layer, to separate redundant modules for additional resiliency.

The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration and reduces errors because most of the commands entered to a port-channel interface are copied to its members interfaces and do not require manual replication.

Configure two or more physical interfaces to be members of the EtherChannel. It is recommended that they are added in multiples of two. Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure traffic is prioritized appropriately.

Not all connected router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet1/0/23
  description Link to RS232-2911-2 Gig0/1
interface GigabitEthernet2/0/23
  description Link to RS232-2911-2 Gig0/2
!
interface range GigabitEthernet1/0/23, GigabitEthernet2/0/23
  switchport
  macro apply EgressQoS
  channel-group 2 mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

**Step 4:** Configure EtherChannel trunk on the access layer switch.

An 802.1Q trunk is used which allows the router to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access layer switch. When using EtherChannel the interface type will be port-channel and the number must match the channel group configured in Step 3. DHCP Snooping and Address Resolution Protocol (ARP) inspection are set to trust.

```
interface Port-channel2
  description EtherChannel link to RS232-2911-2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,69,99
  switchport mode trunk
  ip arp inspection trust
  spanning-tree portfast trunk
  ip dhcp snooping trust
  no shutdown
```

The Catalyst 2960-S and 4500 do not require the **switchport trunk encapsulation dot1q** command.

## Option 2: Layer 2 trunk from router to access layer switch

**Step 1:** Enable the physical interface on the router.

```
interface GigabitEthernet0/2
  description RS232-A2960S Gig1/0/23
  no ip address
  no shutdown
```

**Step 2:** Configure the trunk on the access layer switch.

Use an 802.1Q trunk for the connection, which allows the router to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. DHCP Snooping and Address Resolution Protocol (ARP) inspection are set to trust.

```
interface GigabitEthernet1/0/23
  description Link to RS232-2911-2 Gig0/2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,69,99
  switchport mode trunk
  ip arp inspection trust
  spanning-tree portfast trunk
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  ip dhcp snooping trust
  no shutdown
```

The Catalyst 2960-S and 4500 do not require the `switchport trunk encapsulation dot1q` command.

### Procedure 9 Configure Access Layer Interfaces

**Step 1:** Create subinterfaces and assign VLAN tags.

After the physical interface or port-channel have been enabled, then the appropriate data or voice subinterfaces can be mapped to the VLANs on the LAN switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration. The subinterface portion of the configuration should be repeated for all data or voice VLANs.

```
interface [type] [number] . [sub-interface number]
  encapsulation dot1q [dot1q VLAN tag]
```

**Step 2:** Configure IP settings for each subinterface.

This design uses an IP addressing convention with the default gateway router assigned an IP address and IP mask combination of **N.N.N.1 255.255.255.0** where N.N.N is the IP network and 1 is the IP host.

When you are using a centralized DHCP server, your routers with LAN interfaces connected to a LAN using DHCP for end-station IP addressing must use an IP helper.

This remote-site DMVPN spoke router is the second router of a dual-router design and HSRP is configured at the access layer. The actual interface IP assignments will be configured in the following procedure.

```
interface [type][number].[sub-interface number]
  description [usage]
  encapsulation dot1Q [dot1q VLAN tag]
  ip helper-address 10.4.48.10
  ip pim sparse-mode
```

#### **Example: Layer 2 EtherChannel**

```
interface Port-channel2
  no ip address
  no shutdown
  !
  hold-queue 150 in
  !
interface Port-channel2.64
  description Data
  encapsulation dot1Q 64
  ip helper-address 10.4.48.10
  ip pim sparse-mode
  !
interface Port-channel2.69
  description Voice
  encapsulation dot1Q 69
  ip helper-address 10.4.48.10
  ip pim sparse-mode
```

#### **Example: Layer 2 Link**

```
interface GigabitEthernet0/2
  no ip address
  no shutdown
  !
interface GigabitEthernet0/2.64
  description Data
  encapsulation dot1Q 64
  ip helper-address 10.4.48.10
  ip pim sparse-mode
  !
interface GigabitEthernet0/2.69
  description Voice
  encapsulation dot1Q 69
  ip helper-address 10.4.48.10
  ip pim sparse-mode
```

## Procedure 10 Configure Access Layer HSRP

You configure HSRP to enable a VIP that you use as a default gateway that is shared between two routers. The HSRP active router is the router connected to the primary carrier and the HSRP standby router is the router connected to the secondary carrier or backup link. Configure the HSRP standby router with a standby priority that is lower than the HSRP active router.

The router with the higher standby priority value is elected as the HSRP active router. The preempt option allows a router with a higher priority to become the HSRP active, without waiting for a scenario where there is no router in the HSRP active state. The relevant HSRP parameters for the router configuration are shown in the following table.

Table 31 - WAN remote-site HSRP parameters (Dual Router)

Router	HSRP role	Virtual IP address (VIP)	Real IP address	HSRP priority	PIM DR priority
Primary	Active	.1	.2	110	110
Secondary	Standby	.1	.3	105	105

The dual-router access-layer design requires a modification for resilient multicast. The PIM DR should be on the HSRP active router. The DR is normally elected based on the highest IP address and has no awareness of the HSRP configuration. In this design, the HSRP active router has a lower real IP address than the HSRP standby router, which requires a modification to the PIM configuration. The PIM DR election can be influenced by explicitly setting the DR priority on the LAN-facing subinterfaces for the routers.



### Tech Tip

The HSRP priority and PIM DR priority are shown in the previous table to be the same value; however there is no requirement that these values must be identical.

Repeat this procedure for all data or voice subinterfaces.

```
interface [interface type][number].[sub-interface number]
 ip address [LAN network 1 address] [LAN network 1 netmask]
 ip pim dr-priority 105
 standby version 2
 standby 1 ip [LAN network 1 gateway address]
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string cisco123
```

### Example: Layer 2 EtherChannel

```
interface PortChannel2
 no ip address
 no shutdown
!
interface PortChannel2.64
 description Data
 encapsulation dot1Q 64
```

```

ip address 10.5.212.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.212.1
standby 1 priority 105
standby 1 preempt
standby 1 authentication md5 key-string cisco123
!
interface PortChannel2.69
description Voice
encapsulation dot1Q 69
ip address 10.5.213.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.13.1
standby 1 priority 105
standby 1 preempt
standby 1 authentication md5 key-string cisco123

```

### Example: Layer 2 Link

```

interface GigabitEthernet0/2
no ip address
no shutdown
!
interface GigabitEthernet0/2.64
description Data
encapsulation dot1Q 64
ip address 10.5.212.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.212.1
standby 1 priority 105
standby 1 preempt
standby 1 authentication md5 key-string cisco123
!
interface GigabitEthernet0/2.69
description Voice
encapsulation dot1Q 69
ip address 10.5.213.3 255.255.255.0
ip helper-address 10.4.48.10
ip pim dr-priority 105

```

```
ip pim sparse-mode
standby version 2
standby 1 ip 10.5.13.1
standby 1 priority 105
standby 1 preempt
standby 1 authentication md5 key-string cisco123
```

## Procedure 11 Configure Transit Network

Configure the transit network between the two routers. You use this network for router-router communication and to avoid hairpinning. The transit network should use an additional subinterface on the router interface that is already being used for data or voice.

There are no end stations connected to this network, so HSRP and DHCP are not required.

```
interface [interface type][number].[sub-interface number]
encapsulation dot1q [dot1q VLAN tag]
ip address [transit net address] [transit net netmask]
ip pim sparse-mode
```

### Example

```
interface GigabitEthernet0/2.99
description Transit Net
encapsulation dot1q 99
ip address 10.5.208.2 255.255.255.252
ip pim sparse-mode
```

## Procedure 12 Configure EIGRP (LAN Side)

A routing protocol must be configured between the two routers. This ensures that the HSRP active router has full reachability information for all WAN remote sites.

**Step 1:** Enable EIGRP-100.

You configure EIGRP-100 facing the access layer. In this design, all LAN-facing interfaces and the loopback must be EIGRP interfaces. All interfaces except the transit-network subinterface should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address. Do not include the DMVPN MGRE interface as an EIGRP interface.

```
router eigrp 100
network [network] [inverse mask]
passive-interface default
no passive-interface [Transit interface]
eigrp router-id [IP address of Loopback0]
no auto-summary
```

**Step 2:** Redistribute EIGRP-201 (DMVPN) into EIGRP-100.

EIGRP-201 is already configured for the DMVPN mGRE interface. Routes from this EIGRP process are redistributed. Since the routing protocol is the same, no default metric is required.

```
router eigrp 100
 redistribute eigrp 201
```

### Example

```
router eigrp 100
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 201
 passive-interface default
 no passive-interface GigabitEthernet0/2.99
 eigrp router-id 10.255.254.232
 no auto-summary
```

## Procedure 13 Configure Loopback Resiliency

The remote-site routers have in-band management configured via the loopback interface. To ensure reachability of the loopback interface in a dual-router design, redistribute the loopback of the adjacent router into the WAN routing protocol EIGRP-201 (DMVPN).

**Step 1:** Configure an access list to limit the redistribution to only the adjacent router's loopback IP address.

```
ip access-list standard R[number]-LOOPBACK
 permit [IP Address of Adjacent Router Loopback]
!
route-map LOOPBACK-ONLY permit 10
 match ip address R[number]-LOOPBACK
```

### Example

```
ip access-list standard R1-LOOPBACK
 permit 10.255.253.232
!
route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
```

**Step 2:** Configure EIGRP to redistribute the adjacent router's loopback IP address. The EIGRP stub routing must be adjusted to permit redistributed routes.

```
router eigrp 201
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp stub connected summary redistributed
```

# Deploying a WAN Remote-Site Distribution Layer

## PROCESS

### Remote-Site Router to Distribution Layer

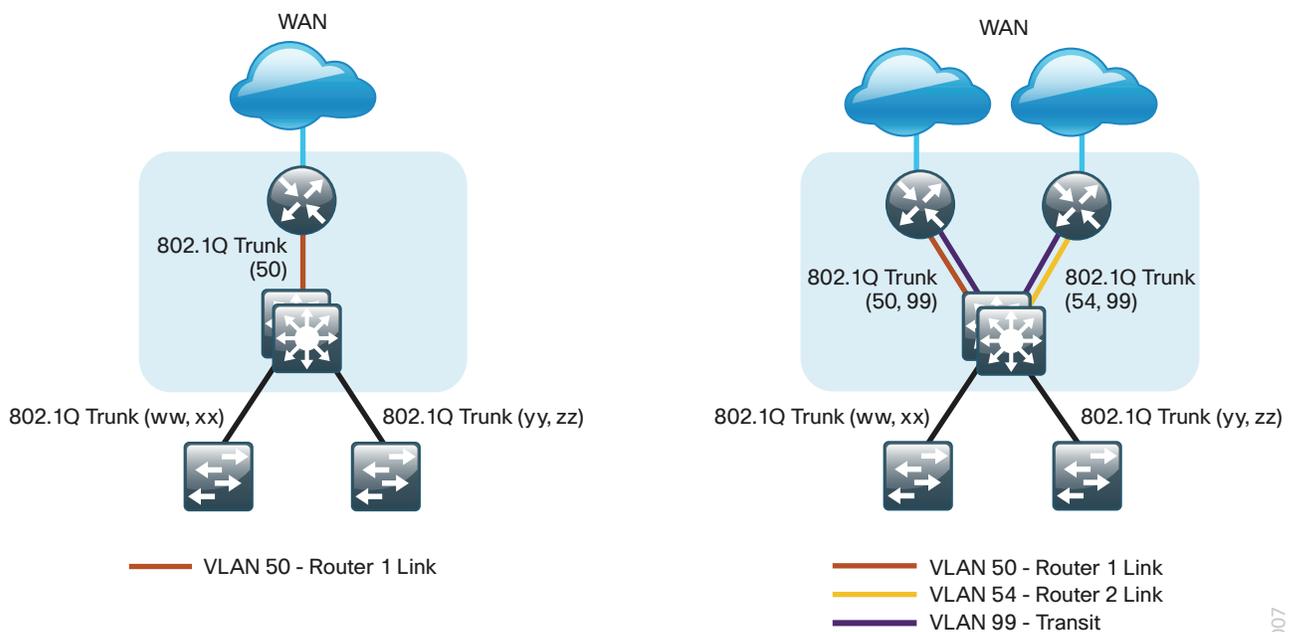
1. Connect Router to Distribution Layer
2. Configure EIGRP (LAN Side)

Use this set of procedures to configure a DMVPN spoke router for a DMVPN remote site (single-router, single-link) and includes all required procedures to connect to a distribution layer.

Also, use this set of procedures for a DMVPN + DMVPN remote site. Use these procedures to connect a distribution layer to a DMVPN spoke router in the single-router, dual-link design. Use these procedures when you are connecting a distribution layer to the first router of the dual-router, dual-link design.

Both distribution layer remote-site options are shown in the following figure.

Figure 26 - WAN remote site - Connection to distribution layer



2007

## Procedure 1 Connect Router to Distribution Layer



### Reader Tip

Please refer to the [Campus Wired LAN Technology Design Guide](#) for complete distribution layer configuration details. This guide only includes the additional steps to complete the distribution layer configuration.

Layer 2 EtherChannels are used to interconnect the CE router to the distribution layer in the most resilient method possible. This connection allows for multiple VLANs to be included on the EtherChannel if necessary.

**Step 1:** Configure port-channel interface on the router.

```
interface Port-channel1
  description EtherChannel link to RS232-D3750X
  no shutdown
```

**Step 2:** Configure the port channel subinterfaces and assign IP addresses.

After you have enabled the interface, map the appropriate subinterfaces to the VLANs on the distribution layer switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration.

The subinterface configured on the router corresponds to a VLAN interface on the distribution-layer switch. Traffic is routed between the devices with the VLAN acting as a point-to-point link.

```
interface Port-channel1.50
  description R1 routed link to distribution layer
  encapsulation dot1Q 50
  ip address 10.5.208.1 255.255.255.252
  ip pim sparse-mode
```

**Step 3:** Configure EtherChannel member interfaces on the router.

Configure the physical interfaces to tie to the logical port-channel using the channel-group command. The number for the port-channel and channel-group must match. Not all router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet0/1
  description RS232-D3750X Gig1/0/1
  !
interface GigabitEthernet0/2
  description RS232-D3750X Gig2/0/1
  !
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

**Step 4:** Configure VLAN on the distribution layer switch.

```
vlan 50
name R1-link
```

**Step 5:** Configure Layer 3 on the distribution layer switch.

Configure a VLAN interface, also known as a switch virtual interface (SVI), for the new VLAN added. The SVI is used for point to point IP routing between the distribution layer and the WAN router.

```
interface Vlan50
ip address 10.5.208.2 255.255.255.252
ip pim sparse-mode
no shutdown
```

**Step 6:** Configure EtherChannel member interfaces on the distribution layer switch.

Connect the router EtherChannel uplinks to separate switches in the distribution layer switches or stack, and in the case of the Cisco Catalyst 4507R+E distribution layer, to separate redundant modules for additional resiliency.

The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration and reduces errors because most of the commands entered to a port-channel interface are copied to its members interfaces and do not require manual replication.

Configure two or more physical interfaces to be members of the EtherChannel. It is recommended that they are added in multiples of two. Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure traffic is prioritized appropriately.

Not all connected router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet1/0/1
description Link to RS232-2911-1 Gig0/1
interface GigabitEthernet2/0/1
description Link to RS232-2911-1 Gig0/2
!
interface range GigabitEthernet1/0/1, GigabitEthernet2/0/1
switchport
macro apply EgressQoS
channel-group 1 mode on
logging event link-status
logging event trunk-status
logging event bundle-status
```

**Step 7:** Configure EtherChannel trunk on the distribution layer switch.

An 802.1Q trunk is used which allows the router to provide the Layer 3 services to all the VLANs defined on the distribution layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the distribution layer switch. When using EtherChannel the interface type will be port-channel and the number must match the channel group configured in Step 3. DHCP Snooping and Address Resolution Protocol (ARP) inspection are set to trust.

```
interface Port-channel1
  description EtherChannel link to RS232-2911-1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 50
  switchport mode trunk
  spanning-tree portfast trunk
  no shutdown
```

The Catalyst 4500 does not require the **switchport trunk encapsulation dot1q** command.

## Procedure 2 > Configure EIGRP (LAN Side)

You must configure a routing protocol between the router and distribution layer.

**Step 1:** Enable EIGRP-100.

Configure EIGRP-100 facing the distribution layer. In this design, all distribution-layer-facing subinterfaces and the loopback must be EIGRP interfaces. All other interfaces should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp 100
  network 10.5.0.0 0.0.255.255
  network 10.255.0.0 0.0.255.255
  passive-interface default
  no passive-interface [interface]
  eigrp router-id [IP address of Loopback0]
  no auto-summary
```

**Step 2:** Redistribute EIGRP-200 (DMVPN-1) into EIGRP-100.

EIGRP-200 is already configured for the DMVPN mGRE interface. Routes from this EIGRP process are redistributed. Because the routing protocol is the same, no default metric is required.

```
router eigrp [as number]
 redistribute eigrp [as number (DMVPN)]
```

### Example

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 200
 passive-interface default
 no passive-interface Port-channel1.50
 eigrp router-id 10.255.253.232
 no auto-summary
```

## PROCESS

### Additional Configuration for Dual Router Design (Router 1)

1. Configure the Transit Network
2. Configure Loopback Resiliency

This process is required when the first router has already been configured using one of the following processes.

In this guide:

- Remote-Site Router to Distribution Layer

In other guides:

- [MPLS WAN Technology Design Guide—Remote-Site Router to Distribution Layer](#)
- [Layer 2 WAN Technology Design Guide—Remote-Site Router to Distribution Layer](#)

### Procedure 1 Configure the Transit Network

Configure the transit network between the two routers. You use this network for router-router communication and to avoid hairpinning. The transit network should use an additional subinterface on the EtherChannel interface that is already used to connect to the distribution layer.

The transit network must be a non-passive EIGRP interface.

There are no end stations connected to this network so HSRP and DHCP are not required. The transit network uses Layer 2 pass through on the distribution layer switch, so no SVI is required.

**Step 1:** Configure the transit net interface on the router.

```
interface Port-channel1.99
  description Transit Net
  encapsulation dot1Q 99
  ip address 10.5.208.9 255.255.255.252
  ip pim sparse-mode
```

**Step 2:** Enable EIGRP on the transit net interface on the router.

```
router eigrp 100
  no passive-interface Port-channel1.99
```

**Step 3:** Configure transit network VLAN on the distribution layer switch.

```
vlan 99
  name Transit-net
```

**Step 4:** Add transit network VLAN to existing distribution layer switch EtherChannel trunk.

```
interface Port-channel1
  switchport trunk allowed vlan add 99
```

## Procedure 2 Configure Loopback Resiliency

The remote-site routers have in-band management configured via the loopback interface. To ensure reachability of the loopback interface in a dual-router design, redistribute the loopback of the adjacent router into the WAN routing protocol EIGRP-200 (DMVPN).

**Step 1:** Configure an access list to limit the redistribution to only the adjacent router's loopback IP address.

```
ip access-list standard R[number]-LOOPBACK
  permit [IP Address of Adjacent Router Loopback]
!
route-map LOOPBACK-ONLY permit 10
  match ip address R[number]-LOOPBACK
```

### Example

```
ip access-list standard R2-LOOPBACK
  permit 10.255.254.232
!
route-map LOOPBACK-ONLY permit 10
  match ip address R2-LOOPBACK
```

**Step 2:** Configure EIGRP to redistribute the adjacent router's loopback IP address. The EIGRP stub routing must be adjusted to permit redistributed routes.

```
router eigrp 200
  redistribute eigrp 100 route-map LOOPBACK-ONLY
  eigrp stub connected summary redistributed
```

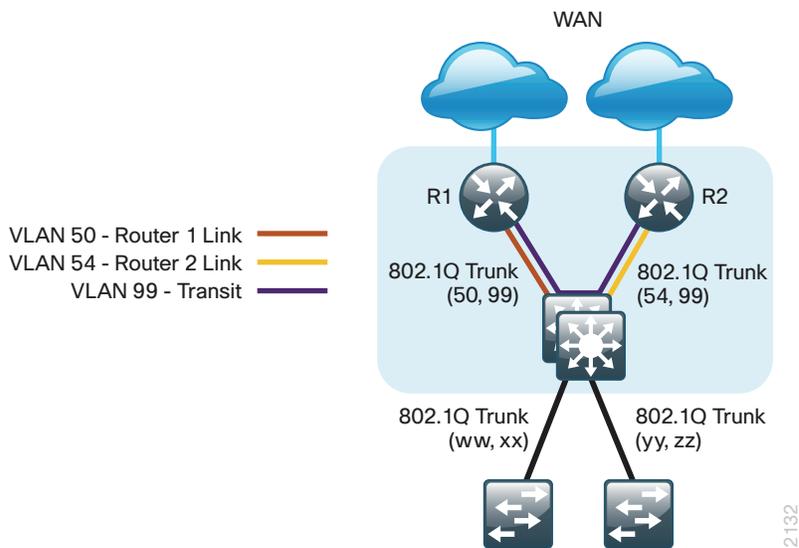
## Remote-Site Router to Distribution Layer (Router 2)

1. Connect Router to Distribution Layer
2. Configure EIGRP (LAN Side)
3. Configure Loopback Resiliency

Use this set of procedures for any of the following topologies: DMVPN + DMVPN remote site, MPLS + DMVPN remote site, or Layer 2 WAN + DMVPN remote site. Use these procedures to connect a distribution layer when configuring the second router of the dual-router, dual-link design. This design uses a separate routed link from the second router of the dual-router scenario to the LAN distribution layer switch.

The dual-router distribution layer remote-site option is shown in the following figure.

Figure 27 - WAN remote site - Connection to distribution layer



### Procedure 1 Connect Router to Distribution Layer



#### Reader Tip

Please refer to the [Campus Wired LAN Design Guide](#) for complete distribution layer configuration details. This guide only includes the additional steps to complete the distribution layer configuration.

Layer 2 EtherChannels are used to interconnect the CE router to the distribution layer in the most resilient method possible. This connection allows for multiple VLANs to be included on the EtherChannel if necessary.

**Step 1:** Configure port-channel interface on the router.

```
interface Port-channel2
  description EtherChannel link to RS232-D3750X
  no shutdown
```

**Step 2:** Configure the port channel subinterfaces and assign IP address.

After you have enabled the interface, map the appropriate subinterfaces to the VLANs on the distribution layer switch. The subinterface number does not need to equate to the 802.1Q tag, but making them the same simplifies the overall configuration.

The subinterface configured on the router corresponds to a VLAN interface on the distribution-layer switch. Traffic is routed between the devices with the VLAN acting as a point-to-point link.

```
interface Port-channel2.54
  description R2 routed link to distribution layer
  encapsulation dot1Q 54
  ip address 10.5.208.5 255.255.255.252
  ip pim sparse-mode
```

**Step 3:** Configure the transit network interface on the router.

```
interface Port-channel2.99
  description Transit Net
  encapsulation dot1Q 99
  ip address 10.5.208.10 255.255.255.252
  ip pim sparse-mode
```

**Step 4:** Configure EtherChannel member interfaces on the router.

Configure the physical interfaces to tie to the logical port-channel using the channel-group command. The number for the port-channel and channel-group must match. Not all router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet0/1
  description RS232-D3750X Gig1/0/2
  !
interface GigabitEthernet0/2
  description RS232-D3750X Gig2/0/2
  !
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 2
  no shutdown
```

**Step 5:** Configure VLAN on the distribution layer switch.

```
vlan 54
  name R2-link
```

**Step 6:** Configure Layer 3 on the distribution layer switch.

Configure a VLAN interface, also known as a switch virtual interface (SVI), for the new VLAN added. The SVI is used for point to point IP routing between the distribution layer and the WAN router.

```
interface Vlan54
  ip address 10.5.208.6 255.255.255.252
  ip pim sparse-mode
  no shutdown
```

**Step 7:** Configure EtherChannel member interfaces on the distribution layer switch.

Connect the router EtherChannel uplinks to separate switches in the distribution layer switches or stack, and in the case of the Cisco Catalyst 4507R+E distribution layer, to separate redundant modules for additional resiliency.

The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration and reduces errors because most of the commands entered to a port-channel interface are copied to its members interfaces and do not require manual replication.

Configure two or more physical interfaces to be members of the EtherChannel. It is recommended that they are added in multiples of two. Also, apply the egress QoS macro that was defined in the platform configuration procedure to ensure traffic is prioritized appropriately.

Not all connected router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet1/0/2
  description Link to RS232-2911-2 Gig0/1
interface GigabitEthernet2/0/2
  description Link to RS232-2911-2 Gig0/2
!
interface range GigabitEthernet1/0/2, GigabitEthernet2/0/2
  switchport
  macro apply EgressQoS
  channel-group 2 mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

**Step 8:** Configure EtherChannel trunk on the distribution layer switch.

An 802.1Q trunk is used which allows the router to provide the Layer 3 services to all the VLANs defined on the distribution layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the distribution layer switch. When using EtherChannel the interface type will be port-channel and the number must match the channel group configured in Step 3. DHCP Snooping and Address Resolution Protocol (ARP) inspection are set to trust.

```
interface Port-channel2
  description EtherChannel link to RS232-2911-2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 54,99
  switchport mode trunk
  spanning-tree portfast trunk
  no shutdown
```

The Catalyst 4500 does not require the **switchport trunk encapsulation dot1q** command.

## Procedure 2 > Configure EIGRP (LAN Side)

You must configure a routing protocol between the router and distribution layer.

**Step 1:** Enable EIGRP-100 on the remote site router.

EIGRP-100 is configured facing the distribution layer. In this design, all distribution-layer-facing subinterfaces and the loopback must be EIGRP interfaces. All other interfaces should remain passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements. This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp 100
  network 10.5.0.0 0.0.255.255
  network 10.255.0.0 0.0.255.255
  passive-interface default
  no passive-interface [routed link interface]
  no passive-interface [transit net interface]
  eigrp router-id [IP address of Loopback0]
  no auto-summary
```

**Step 2:** Redistribute EIGRP-201 (DMVPN-2) into EIGRP-100 on the remote site router.

EIGRP-201 is already configured for the DMVPN mGRE interface. Routes from this EIGRP process are redistributed. Because the routing protocol is the same, no default metric is required.

```
router eigrp [as number]
 redistribute eigrp [as number (DMVPN)]
```

### Example

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 201
 passive-interface default
 no passive-interface Port-channel2.54
 no passive-interface Port-channel2.99
 eigrp router-id 10.255.254.232
 no auto-summary
```

**Step 3:** Enable EIGRP on distribution layer switch VLAN interface.

EIGRP is already configured on the distribution layer switch. The VLAN interface that connects to the router must be configured as a non-passive EIGRP interface.

```
router eigrp 100
 no passive-interface Vlan54
```

## Procedure 3 Configure Loopback Resiliency

The remote-site routers have in-band management configured via the loopback interface. To ensure reachability of the loopback interface in a dual-router design, redistribute the loopback of the adjacent router into the WAN routing protocol EIGRP-201 (DMVPN).

**Step 1:** Configure an access list to limit the redistribution to only the adjacent router's loopback IP address.

```
ip access-list standard R[number]-LOOPBACK
 permit [IP Address of Adjacent Router Loopback]
!
route-map LOOPBACK-ONLY permit 10
 match ip address R[number]-LOOPBACK
```

### Example

```
ip access-list standard R1-LOOPBACK
 permit 10.255.253.232
!
route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
```

**Step 2:** Configure EIGRP to redistribute the adjacent router's loopback IP address. The EIGRP stub routing must be adjusted to permit redistributed routes.

```
router eigrp 201  
  redistribute eigrp 100 route-map LOOPBACK-ONLY  
  eigrp stub connected summary redistributed
```

# Deploying WAN Quality of Service

## PROCESS

### QoS Configuration

1. Create the QoS Maps to Classify Traffic
2. Add ISAKMP Traffic to Network-Critical
3. Define Policy Map to Use Queuing Policy
4. Configure Physical Interface S&Q Policy
5. Apply WAN QoS Policy to Physical Interface
6. Configure IPSEC anti-replay window size

When configuring the WAN-edge QoS, you are defining how traffic egresses your network. It is critical that the classification, marking, and bandwidth allocations align to the service provider offering to ensure consistent QoS treatment end to end.

#### Procedure 1 Create the QoS Maps to Classify Traffic

This procedure applies to all WAN routers.

Use the **class-map** command to define a traffic class and identify traffic to associate with the class name. These class names are used when configuring policy maps that define actions you want to take against the traffic type. The **class-map** command sets the match logic. In this case, the match-any keyword indicates that the maps match any of the specified criteria. This keyword is followed by the name you want to assign to the class of service. After you have configured the **class-map** command, you define specific values, such as DSCP and protocols to match with the match command. You use the following two forms of the **match** command: **match dscp** and **match protocol**.

Use the following steps to configure the required WAN class-maps and matching criteria.

**Step 1:** Create the class maps for DSCP matching.

Repeat this step to create a class-map for each of the six WAN classes of service listed in the following table.

You do not need to explicitly configure the default class.

```
class-map match-any [class-map name]
  match dscp [dscp value] [optional additional dscp value(s)]
```

Table 32 - QoS classes of service

Class of service	Traffic type	DSCP values	Bandwidth %	Congestion avoidance
VOICE	Voice traffic	ef	10 (PQ)	–
INTERACTIVE-VIDEO	Interactive video (video conferencing)	cs4, af41	23 (PQ)	–
CRITICAL-DATA	Highly interactive (such as Telnet, Citrix, and Oracle thin clients)	af31, cs3	15	DSCP based
DATA	Data	af21	19	DSCP based
SCAVENGER	Scavenger	af11, cs1	5	–
NETWORK-CRITICAL	Routing protocols. Operations, administration and maintenance (OAM) traffic.	cs6, cs2	3	–
default	Best effort	Other	25	random

### Example

```
class-map match-any VOICE
  match dscp ef
!
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4 af41
!
class-map match-any CRITICAL-DATA
  match dscp af31 cs3
!
class-map match-any DATA
  match dscp af21
!
class-map match-any SCAVENGER
  match dscp af11 cs1
!
class-map match-any NETWORK-CRITICAL
  match dscp cs6 cs2
```



### Tech Tip

You do not need to configure a Best-Effort Class. This is implicitly included within class-default as shown in Procedure 4.

## Procedure 2 Add ISAKMP Traffic to Network-Critical

For a WAN connection using DMVPN, you need to ensure proper treatment of ISAKMP traffic in the WAN. To classify this traffic requires the creation of an access-list and the addition of the access-list name to the NETWORK-CRITICAL class-map created in Procedure 1.

This procedure is only required for a WAN-aggregation DMVPN hub router or a WAN remote-site DMVPN spoke router.

**Step 1:** Create the access-list.

```
ip access-list extended ISAKMP
  permit udp any eq isakmp any eq isakmp
```

**Step 2:** Add the match criteria to the existing NETWORK-CRITICAL class-map.

```
class-map match-any NETWORK-CRITICAL
  match access-group name ISAKMP
```

## Procedure 3 Define Policy Map to Use Queuing Policy

This procedure applies to all WAN routers.

The WAN policy map references the class names you created in the previous procedures and defines the queuing behavior along with the maximum guaranteed bandwidth allocated to each class. This specification is accomplished with the use of a policy-map. Then, each class within the policy map invokes an egress queue, assigns a percentage of bandwidth, and associates a specific traffic class to that queue. One additional default class defines the minimum allowed bandwidth available for best effort traffic.

### Tech Tip

The local router policy maps define seven classes while most service providers offer only six classes of service. The NETWORK-CRITICAL policy map is defined to ensure the correct classification, marking, and queuing of network-critical traffic on egress to the WAN. After the traffic has been transmitted to the service provider, the network-critical traffic is typically remapped by the service provider into the critical data class. Most providers perform this remapping by matching on DSCP values cs6 and cs2.

**Step 1:** Create the parent policy map.

```
policy-map [policy-map-name]
```

Steps 2-6 are repeated for each class in Table 26 including class-default.

**Step 2:** Apply the previously created class-map.

```
class [class-name]
```

**Step 3:** (Optional) Assign the maximum guaranteed bandwidth for the class.

```
bandwidth percent [percentage]
```

**Step 4:** (Optional) Define the priority queue for the class.

```
priority percent [percentage]
```

**Step 5:** (Optional) Define the congestion mechanism.

```
random-detect [type]
```

### Example

```
policy-map WAN
  class VOICE
    priority percent 10
  class INTERACTIVE-VIDEO
    priority percent 23
  class CRITICAL-DATA
    bandwidth percent 15
    random-detect dscp-based
  class DATA
    bandwidth percent 19
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 5
  class NETWORK-CRITICAL
    bandwidth percent 3
  class class-default
    bandwidth percent 25
    random-detect
```



### Tech Tip

Although these bandwidth assignments represent a good baseline, it is important to consider your actual traffic requirements per class and adjust the bandwidth settings accordingly.

## Procedure 4 Configure Physical Interface S&Q Policy

With WAN interfaces using Ethernet as an access technology, the demarcation point between the enterprise and service provider may no longer have a physical-interface bandwidth constraint. Instead, a specified amount of access bandwidth is contracted with the service provider. To ensure the offered load to the service provider does not exceed the contracted rate that results in the carrier discarding traffic, you need to configure shaping on the physical interface. This shaping is accomplished with a QoS service policy. You configure a QoS service policy on the outside Ethernet interface, and this parent policy includes a shaper that then references a second or subordinate (child) policy that enables queuing within the shaped rate. This is called a hierarchical Class-Based Weighted Fair Queuing (HCBWFQ) configuration. When you configure the **shape average** command, ensure that the value matches the contracted bandwidth rate from your service provider.

This procedure applies to all WAN routers. You can repeat this procedure multiple times to support devices that have multiple WAN connections attached to different interfaces.

**Step 1:** Create the parent policy map.

As a best practice, embed the interface name within the name of the parent policy map.

```
policy-map [policy-map-name]
```

**Step 2:** Configure the shaper.

```
class [class-name]
  shape [average | peak] [bandwidth (kbps)]
```

**Step 3:** Apply the child service policy.

```
service-policy [policy-map-name]
```

## Example

This example shows a router with a 20-Mbps link on interface GigabitEthernet0/0 and a 10-Mbps link on interface GigabitEthernet0/1.

```
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 20000000
  service-policy WAN
!
policy-map WAN-INTERFACE-G0/1
  class class-default
    shape average 10000000
  service-policy WAN
```

## Procedure 5 Apply WAN QoS Policy to Physical Interface

To invoke shaping and queuing on a physical interface, you must apply the parent policy that you configured in the previous procedure.

This procedure applies to all WAN routers. You can repeat this procedure multiple times to support devices that have multiple WAN connections attached to different interfaces.

**Step 1:** Select the WAN interface.

```
interface [interface type] [number]
```

**Step 2:** Apply the WAN QoS policy.

The service policy needs to be applied in the outbound direction.

```
service-policy output [policy-map-name]
```

## Example

```
interface GigabitEthernet0/0
  service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
  service-policy output WAN-INTERFACE-G0/1
```

**(Optional)**

Cisco IOS provides anti-replay protection against an attacker duplicating encrypted packets.

IPsec security association (SA) anti-replay is a security service in which the decrypting router can reject duplicate packets and protect itself against replay attacks.

Cisco QoS gives priority to high-priority packets. This prioritization may cause some low-priority packets to be discarded. By expanding the IPsec anti-replay window you can allow the router to keep track of more than 64 packets.

**Step 1:** Increase the anti-replay window size.

```
crypto ipsec security-association replay window-size 1024
```

**Tech Tip**

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed.

It is recommended that you use the full 1024 window size to eliminate future anti-replay problems.

If you do not increase the window size, the router may drop packets and you may see the following error message on the router CLI:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

On the Cisco ASR 1000 router platform, the maximum replay window size is 512.

```
crypto ipsec security-association replay window-size 512
```

# Appendix A: Product List

## WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco ISR 4451-X Security Bundle w/SEC license PAK	ISR4451-X-SEC/K9	15.3(3)S securityk9 license
	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.2(4)M4 securityk9 license datak9 license
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	

## WAN Aggregation

Functional Area	Product Description	Part Numbers	Software
WAN-aggregation Router	Aggregation Services 1002X Router	ASR1002X-5G-VPNK9	IOS-XE 15.3(3)S Advanced Enterprise license
	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
WAN-aggregation Router	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.2(4)M4 securityk9 license datak9 license
	Cisco 3925 Security Bundle w/SEC license PAK	CISCO3925-SEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	

## Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1) IPS 7.1(7) E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

## Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	15.0(2)SE2 IP Base license

## LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) IP Base license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.2.1SE(15.0-1EX1) IP Base license
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE2 LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

## LAN Distribution Layer

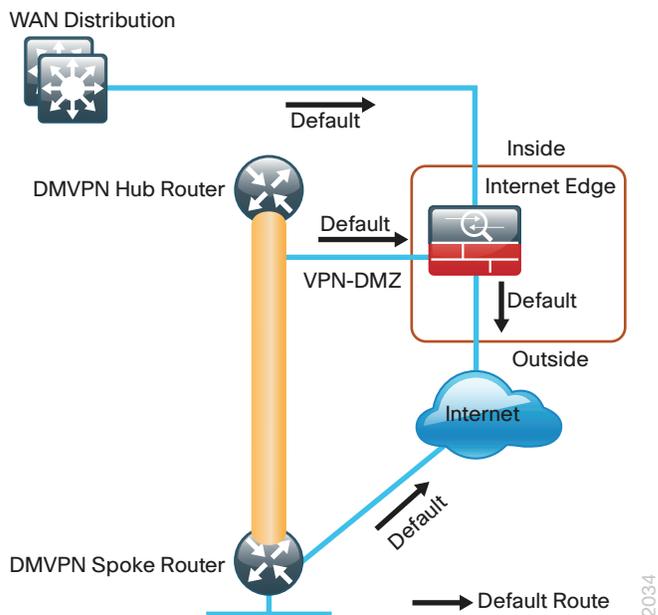
Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.1(1)SY IP services license
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) Enterprise Services license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE2 IP Services license
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

# Appendix B: Technical Feature Supplement

## Front Door VRF (FVRF) for DMVPN

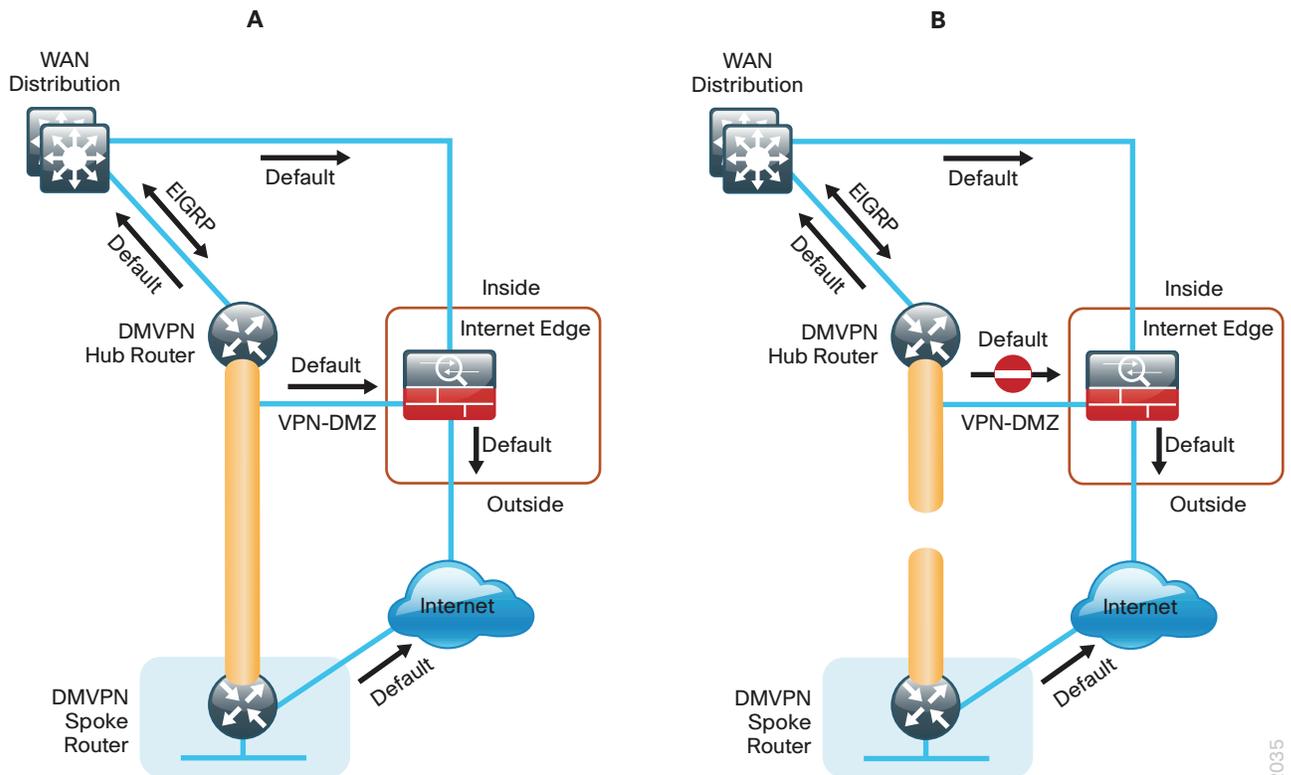
Building an IPsec tunnel requires reachability between the crypto routers. When you use the Internet, routers use a default route to contact their peers.

Figure 28 - IPsec tunnel



If you need to extend the internal network (and the same default routing options that are available to internal users), you must advertise a default route to the VPN hub router. For details, see section A in the following figure.

Figure 29 - IPsec tunnel before/after default route injection



The advertisement of a default route to the hub router (with an existing default route) is problematic. This route requires a better administrative distance to become the active default, which then overrides the default route that is supporting the peer-to-peer IPsec tunnel connection. This routing advertisement breaks the tunnel as shown in section B in the previous figure.

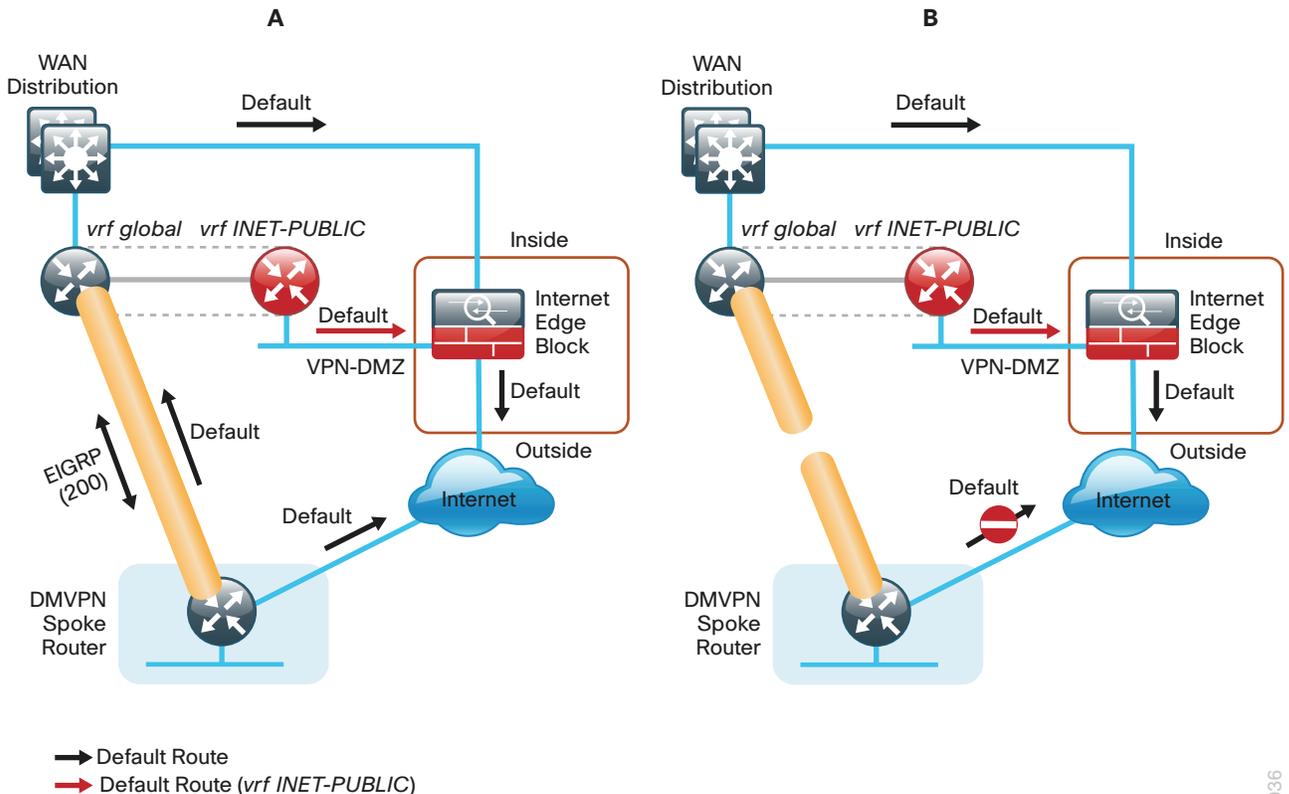
2035

Through the introduction of an external VRF INET-PUBLIC (shown in red), the hub router can support multiple default routes. The internal network remains in the global VRF. This is shown in section A of the following figure.

**i** Tech Tip

Most additional features on the hub router do not require VRF-awareness.

Figure 30 - IPsec tunnel with FVRF aggregation



2036

This configuration is referred to as FVRF, because the Internet is contained in a VRF. The alternative to this design is inside VRF (IVRF), where the internal network is in a VRF on the VPN hub and the Internet remains in the global VRF. This method is not documented in this guide.

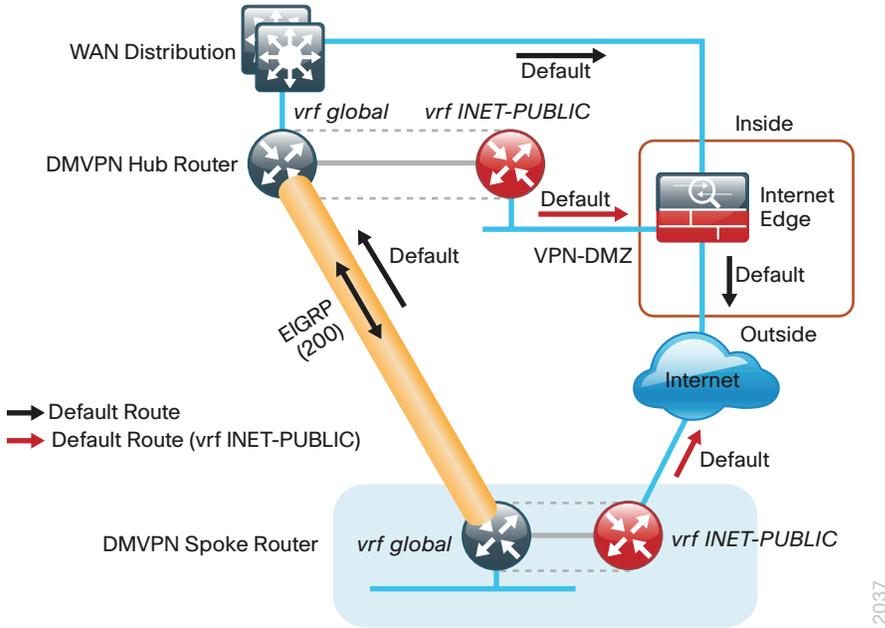
It is now possible to reestablish the IPsec tunnel to the remote peer router. As the remote-site policy requires central Internet access for end users, a default route is advertised through the tunnel. This advertisement causes a similar default routing issue on the remote router; the tunnel default overrides the Internet-pointing default and the tunnel connection breaks as shown in section B of the previous figure.

This configuration requires using FVRF on the remote-site router as well. The primary benefits of using this solution are as follows:

- Simplified default routing and static default routes in the INET-PUBLIC VRFs
- Ability to support default routing for end-users traffic through VPN tunnels
- Ability to use dynamic default routing for sites with multiple WAN transports
- Ability to build spoke-to-spoke tunnels with DMVPN with end-user traffic routed by default through VPN tunnels

The final design that uses FVRF at both the WAN-aggregation site and a WAN remote-site is shown in the following figure.

Figure 31 - FVRF—Final configuration



# Appendix C: Device Configuration Files

---

To view the configuration files from the CVD lab devices that we used to test this guide, please go to the following URL:

<http://cvddocs.com/fw/330-13>

# Appendix D: Changes

---

This appendix summarizes the changes to this guide since its last edition.

- Added support for Cisco 4451-X Integrated Services Router platform
- Added a WAN facing summary route for the remote-site network range. The summary route ensures that default routing changes do not affect remote-site communication between WAN transports.
- Added configuration to adjust IPsec anti-replay window size.

## Feedback

Please use the [feedback form](#) to send comments and suggestions about this guide.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)